ILLICIT USE OF VIRTUAL CURRENCY AND THE LAW ENFORCEMENT RESPONSE

HEARING

BEFORE THE

SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

JUNE 20, 2018

Printed for the use of the Committee on Financial Services

Serial No. 115–102

U.S. GOVERNMENT PUBLISHING OFFICE
31–491 PDF WASHINGTON : 2019

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
THOMAS MACARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
CHARLIE CRIST, Florida
RUBEN KIHUEN, Nevada

SHANNON MCGAHN, *Staff Director*

SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

STEVAN PEARCE, New Mexico *Chairman*

ROBERT PITTENGER, North Carolina, *Vice Chairman*
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee

ED PERLMUTTER, Colorado, *Ranking Member*
CAROLYN B. MALONEY, New York
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
RUBEN KIHUEN, Nevada
STEPHEN F. LYNCH, Massachusetts

CONTENTS

ILLICIT USE OF VIRTUAL CURRENCY AND THE LAW ENFORCEMENT RESPONSE

Wednesday, June 20, 2018

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TERRORISM
AND ILLICIT FINANCE,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:04 p.m., in room 2128, Rayburn House Office Building, Hon. Stevan Pearce [chairman of the subcommittee] presiding.

Present: Representatives Pearce, Pittenger, Tipton, Poliquin, Zeldin, Davidson, Budd, Maloney, Himes, Foster, Delaney, Sinema, Vargas, Gottheimer, and Waters.

Also present: Representatives Scott, Velazquez, Crist, Heck, and Capuano.

Chairman PEARCE. The subcommittee will come to order. Without objection, the Chair is authorized to declare a recess with the subcommittee at any time. Members of the full committee who are not Members of the Subcommittee on Terrorism and Illicit Finance may participate in today's hearing. All Members will have 5 legislative days within which to submit extraneous materials to the Chair for inclusion in the record.

This hearing is entitled, "Illicit Use of Virtual Currency and the Law Enforcement Response." I now recognize myself for 3 minutes to give an opening statement.

I want to thank everyone for joining us today. Today's hearing is going to examine the exploitation of virtual currencies and how law enforcement is working to identify and disrupt their use to fund illicit activities through both mainstream and dark Web marketplaces. With today's advancements in the evolving world of financial technology, the ability to deposit, transfer, and raise money is at our fingertips. While this is a significant improvement for those who struggle to access the financial system, the ease of transacting also opens the doorway for abuse by bad actors.

The appeal of virtual currencies to criminals is their ability to transact across the globe and the low cost of resolution. Virtual currencies are also well known for being the preferred means to purchase drugs, illicit goods, and criminal services from online forums on the dark Web, including places like the Silk Road and AlphaBay. There is also anecdotal evidence of terrorist groups transferring money and attempting to raise funds using virtual currencies.

Moving forward, as this technology becomes cheaper and more prevalent globally, we must be aware of the risks, the abuse of the virtual currencies can pose to our financial system, criminal groups infect computers and networks with ransomware and ask for payments in virtual currency or use online marketplaces to buy, sell, and advertise illicit goods and services.

As Members of Congress, we should work to remain as informed as possible about the current and emerging risks around us. And in fact, Members of this subcommittee have already been active in this arena. Last week, I was happy to speak in support of the FIND Trafficking Act, a bill that would require the Government Accountability Office to study and report how virtual currencies in online marketplaces can be used for illicit means. This bill is a first step in defining the issues surrounding virtual currency exploitation, as well as creating solutions to help law enforcement and protect our citizens.

I also applaud Congressman Ted Budd for introducing the Financial Technology Protection Act earlier this year, which would bring industry insiders and Federal regulators together to find best practices and solutions to help our law enforcement solve this problem.

Today's hearing is an opportunity to learn more about law enforcement's investigations and responses to the illicit use of virtual currencies. I hope our Members will take this chance to learn from our witnesses about the current issues facing law enforcement in the detection of criminal activity in this area and explore what additional tools may be necessary to combat threats to the U.S. financial system. We would also like to thank our witnesses for being here today. I look forward to your testimony.

I would now recognize Mr. Foster for 5 minutes.

Mr. FOSTER. Thank you, Chairman Pearce and thank you to our witnesses here.

The illicit use of virtual currency is a very important topic. And under normal circumstances, I would say that it deserves our full attention. However, there are extraordinary circumstances today. Hundreds of children are sitting in cages who have been forcibly separated from their families. And so, I think this is really the issue that is more pressing to discuss.

Mr. Nevano, as the highest ranking ICE (U.S. Immigration and Customs Enforcement) official who is being allowed to testify before Congress, we Democrats have some questions that we will be asking you. Just last month, ICE agents rounded up and incarcerated immigrants, as well as people who simply appeared to look like immigrants to them, in and around my district in Illinois and without any apparent cause or reason and uncertain attention paid to adequate rules and procedures.

On our southern border, ICE agents are ripping children out of their parents' arms. We don't need a new law to put an end to this trauma and the President could very easily have put a stop to any of these policies with one phone call a week ago or simply never have put these policies in place at all. Instead, he chose to manufacture a humanitarian crisis that was unnecessary and easily preventable.

The United States has served as a beacon of hope and freedom since its founding. We are watching that hope and freedom erode

right before our eyes as thousands of these children spend another night in a metal cage.

Mr. Nevano, history does not look kindly on our government when we do not uphold our commitment to human rights and basic morality. I strongly believe that the American people deserve a government that embodies the values on which it was founded. We look forward to your testimony and the answers that you will be providing to this committee.

Thank you. I yield back.

Chairman PEARCE. I now recognize the gentleman from North Carolina, Mr. Pittenger, for 2–1/2 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman and Ranking Member Perlmutter for your leadership and holding this hearing today.

Additionally, I would also like to thank our distinguished panelists for lending their expertise to our subcommittee this afternoon. Of special note is Financial Services intern and UVA student, Hugo Bonilla, for his exceptional research on virtual currencies.

One of the greatest emerging threats to U.S. national security is illicit use of virtual or cryptocurrencies. Domestic and international law enforcement agencies have begun taking the steps necessary to combat this new model of criminal transactions. It is our duty to provide the tools and the oversight of said tools required to maintain our edge over our adversaries.

Virtual currency, due to its higher degree of anonymity, is seen as a very lucrative opportunity for those with nefarious intentions. The risk that arises from this anonymity is that criminals can use virtual currencies to store and transmit their financial gains from illegal practices such as drug dealing or human trafficking. Under the guidance of the Department of Homeland Security (DHS), the Secret Service, and the National Computer Forensics Institute, they provided our State and local law enforcement personnel with the training necessary to investigate and combat cyber crime, including the illicit use of virtual currency. And issues like these must be continued and expanded by Congress to combat this emerging threat.

I have hosted a dozen parliamentary intelligence security forums over the last 5 years in which delegates from 68 nations have met to address issues such as this. The United States must continue acting as a global leader in the realm of cybersecurity. It is my hope that today we can thoroughly examine this threat to determine what additional tools and resources we need to combat it.

Thank you, Mr. Chairman. I yield back the balance of my time.

Chairman PEARCE. The gentleman yields back.

The Chair would now recognize the gentlelady from California, Ms. Waters, for 3 minutes.

Ms. WATERS. Thank you very much. Thank you for scheduling today's hearing to examine the illicit uses of virtual currency and the law enforcement response. It is alarming how virtual currencies, especially newer ones, are being used to finance terrorism, launder money, and purchase drugs and weapons on the dark Web.

This is an important topic. However, it is not the only topic that we must discuss today. Despite the fact that the witness from the Department of Homeland Security works for U.S. Immigration and Customs Enforcement, commonly known as ICE, and is not the

agency tasked with working on the border, it would be a dereliction of duty if I did not share my concerns about the human rights abuses occurring on our border at President Trump's direction and at least find out what ICE's role is in this issue.

The world has watched and listened in horror and with overwhelming sadness as children have been ripped from their parents and separated from their families. They are young, alone, and terrified without their families and made to live in literal cages. It is not clear when this child abuse will end.

The White House has made every argument it can to deflect the blame for their zero tolerance policy that led to the forcible separation of over 2,000 children from their parents in just 6 weeks. They have quoted the Bible, denied the policy, and begrudgingly acknowledged it. The President, in an attempt to convince the American public that up is down and down is up, even tried to blame Democrats for his own policy.

This is Donald Trump's abhorrent policy. This is child abuse. Neither of those statements is refutable. It is time for the President, Department of Homeland Security Secretary Nielsen, and Department of Justice Attorney General Sessions to admit that their actions were not thought out and that the consequences of those actions are inhumane and completely inconsistent with the values of this country.

And I am hoping that during the period where we can raise some questions that you will be able to help us understand what your role is. And with that, I yield back the balance of my time.

Chairman PEARCE. The gentlelady yields back.

The Chair now welcomes the testimony of our two witnesses. The third is stuck in traffic reportedly somewhere on New York. I am assuming that is the avenue, not the city. But we will introduce Mr. Ott when he comes. He is representing FinCEN here today.

Mr. Robert Novy is a Deputy Assistant Director of the United States Secret Service Office of Investigations with oversight of criminal investigations, operations, strategy, and policy related to cyber and financial crimes. Mr. Novy was detailed with the staff of the National Security Council at the White House as the Director for Cyber Security Incident Response, Intelligence, and Defense Policy and was the deputy assistant director for the Congressional Affairs and special agent in charge for public affairs.

Mr. Novy has previously served as the supervisor of the Electronic Crimes Task Force in the New York Field Office and was a member of the Washington Field Office's Electronic Crimes Special Agent Program. In addition to his expertise on cyber crime, Mr. Novy served on the Presidential Protective Division during both the Clinton and Bush Administrations. Prior to his Secret Service career, Mr. Novy was an assistant branch chief for the U.S. Securities and Exchange Commission (SEC), also served in the U.S. Navy.

Mr. Novy received his Masters of Public Administration from Troy State University and serves on the Board of Advisers for the University of Texas in Austin.

Mr. Gregory Nevano is a Deputy Assistant Director at Homeland Security Investigations Illicit Trade, Travel, and Finance Division with oversight of all financial, narcotics, document and benefit

fraud, criminal gang exploitation, and several targeting infusion centers. Previously, Mr. Nevano served as the chief of staff to the deputy director of the U.S. Immigration Customs and Enforcement, ICE, as the associate deputy assistant director for the Investigative Services Division and is the unit chief for the Asset Forfeiture Unit.

Mr. Nevano's long career also included assignments as an assistant special agent in charge in the ICE Boston Field Office, the group supervisor of the Narcotics and Violent Gang Group—or group supervisor of the Operational Support Group as a detailee to the FBI's Joint Terrorism Task Force. Mr. Nevano received his Bachelors of Science in political science from Boston College.

We will go ahead and introduce Mr. Ott and we will then just move into his testimony when he comes. But he is the Associate Director for the Financial Crimes Enforcement Network or FinCEN's Enforcement Division with oversight of the FinCEN Bank Secrecy Act (BSA) Compliance and Enforcement Program. Mr. Ott joined FinCEN in 2014 as a senior adviser to the director and was responsible for providing guidance on various matters regarding law enforcement and transnational crime.

Prior to joining FinCEN, Mr. Ott was a prosecutor for over 25 years with both the Tax and Criminal Divisions of the United States Department of Justice, most recently serving for 8 years as deputy chief of the Organized Crime and Racketeering Section. Throughout Mr. Ott's career with the DOJ, he prosecuted and supervised prosecutions of cases involving RICO, public corruption, national security, tax evasion, financial fraud, and money laundering. Mr. Ott received his juris doctorate degree from the University of Baltimore School of Law.

Each of you will now be recognized for 5 minutes to give an oral presentation of your testimony. Without objection, each of your written statements will be made part of the record.

Mr. Nevano, you are recognized for 5 minutes.

STATEMENT OF GREGORY NEVANO

Mr. NEVANO. Chairman Pearce, Ranking Member Perlmutter, distinguished Members, and my fellow law enforcement colleagues, thank you for the opportunity to appear before you today to discuss the use of virtual currency and the efforts of U.S. Immigration and Customs Enforcement to target and investigate those who exploit virtual currency to carry out nefarious activity.

ICE's Homeland Security Investigations (HSI) has long stood at the forefront of combating transnational criminal activity that seeks to exploit our trade, travel, and financial systems for illicit purposes. HSI is the largest investigative agency within the U.S. Department of Homeland Security with more than 6,000 special agents assigned to more than 200 domestic offices and 67 international offices in 50 countries. HSI has the authority to enforce more than 400 U.S. Federal statutes to include financial crimes and the use of virtual currency.

Virtual currency is not a new phenomenon. Virtual currency, in the form of airline mileage reward programs, has been in existence since the early 1980's. The challenge for law enforcement; however, began in 2009, when Bitcoin was introduced as the first decentral-

ized virtual currency. With its introduction, an entirely new world was created in relation to money laundering and financial investigations. Following its introduction, Bitcoin quickly became the currency of choice on the dark Net as buyers and sellers enjoyed the pseudo-anonymity it provided.

The good news for law enforcement; however, is that despite the pseudo-anonymity exploited by the use of Bitcoin and other virtual currencies, as well as their ease to transfer at some point, criminals need to convert their cash into virtual currency or their virtual currency into cash. Whenever monetary exchanges are made, a choke point is created. This is the time when criminals are most vulnerable and can be identified by law enforcement means and methods.

Utilizing the traditional investigative methods coupled with financial and blockchain analysis, HSI is able to disrupt and dismantle the criminals and the TCOs utilizing virtual currencies. Legitimate users of virtual currencies are more than willing to conduct business with a legitimate virtual currency exchange. Legitimate exchanges are registered with the U.S. Department of Treasury's Finance Crimes Enforcement Network also known as FinCEN.

FinCEN issued guidance in 2013 identifying persons or companies involved in the exchange of virtual currency as money service businesses, requiring them to follow regulatory and reporting protocols. Those who use virtual currency for illegal purposes; however, more often than not stay away from registered exchanges in an attempt to conceal their own identities. Instead, these criminals look to illicit or unregistered peer-to-peer exchanges that don't require or ask for personal identifying information. They illegally generate revenue by charging a premium for allowing their customers to remain anonymous. They will sell cryptocurrencies above market value and buy below market value from those customers who wish to remain anonymous.

As part of the commitment to combating the opioid crisis in the United States, HSI has engaged in a multiyear effort to increase its cyber-enabled workforce by training employees to conduct online investigations. Additionally, HSI has conducted virtual currency and dark Net training for Federal, State, local, tribal, and international partners. In Fiscal Year 2018, HSI has conducted more than 50 outreach and training sessions both nationally and internationally reaching over 4,000 law enforcement partners.

HSI not only collaborates with fellow law enforcement agencies, we also understand the importance of partnering with the private industry. We expanded the focus of Operation Cornerstone which was created in 2003, with a primary focus and goal of detecting and closing vulnerabilities within the U.S. financial, trade, and transportation sectors. With the rapid growth of virtual currency and with the expansion of private companies involved in virtual currency, HSI has expanded Operation Cornerstone to include private industry involved in the virtual currency space.

HSI's increased commitment to conducting virtual currency investigations has steadily increased as evidenced by our increase in training and collaboration. In Fiscal Year 2011, HSI initiated only one investigation of virtual currency. However, by 2017, we initi-

ated 203. As of May 2018, HSI has already initiated 144 virtual currency investigations. With the increase in our investigations, HSI has also seen a large increase in our seizures.

For example, in FY 2014, HSI seized 150,000 in virtual currency. However, by the end of Fiscal Year 2017, we seized nearly 7 million in virtual currency. And right now, in this Fiscal Year through April 2018, HSI has already seized more than 25 million in virtual currency. Technology will inevitably continue to evolve and law enforcement agencies everywhere must continue to adapt and evolve as well. HSI will continue to partner with all law enforcement agencies along with cutting-edge technology partners.

In closing, I appreciate your interest in the bourgeoning field of virtual currency and thank you again for the opportunity to appear before you today. I look forward to answering any of your questions.

[The prepared statement of Mr. Nevano can be found on page 34 of the Appendix.]

Chairman PEARCE. Thank you.

Mr. Novy, you are recognized for 5 minutes.

STATEMENT OF ROBERT NOVY

Mr. NOVY. Chairman Pearce, Ranking Member Perlmutter, and Members of the subcommittee, thank you for allowing me to testify today.

The challenge of the illicit use of digital currency spans across sectors of industry and areas of criminal law. As such, the response necessarily requires a whole of government approach. That is why I am so pleased to be here today with two of our partners from FinCEN and ICE. I would like to commend them for their important work and for continuing their productive partnership with us at the United States Secret Service.

At its most basic level, the challenge of digital currencies mirror those challenges faced by the broader financial system. The key to success in countering crime is to identify the beneficiary of the crime. So, that is why we follow the money. This rule has held true for thousands of years and continues for crimes in cyberspace and crimes involving digital currencies.

As one of the Nation's original investigative agencies, the United States Secret Service has, for over 150 years, conducted criminal investigations to protect the American public, financial institutions, and critical infrastructure from criminal exploitation. In 1982, the Secretary of Treasury directed us to investigate crimes related to electronic funds transfer. Two years later in 1984, Congress passed legislation to expand the Secret Service's responsibilities to include investigating a range of computer hacking and access device violations. And today, we have extensive authorities to safeguard financial and payment systems from criminal exploitation, especially from those enabled by the Internet.

To perform our mission, the United States Secret Service has long kept pace with new technologies used by the financial sector. Accordingly, over the past 30 years, we have successfully investigated and arrested some of the world's most significant and most sophisticated cyber criminals. Today, with respect to digital currencies, our primary focus is around three core areas: No. 1, crimi-

nal schemes that undermine the integrity of the financial systems; No. 2, money laundering; and, No. 3, fraud schemes that include computer access device, identity theft, and other forms of fraud.

Over the past decade, working with our law enforcement partners here and around the world, we have investigated and shut down two major centralized digital currencies, both of which supported extensive criminal activity: eGold in 2007 and Liberty Reserve in 2013. The Secret Service continues to work on a range of investigations involving digital currencies. A few of these cases are referenced in my written testimony.

Let me stress, there are real and legitimate commercial applications for digital currencies. That said, in recent years, some digital currencies have been widely adopted for illicit purposes. For example, eGold and Liberty Reserve, two centralized digital currencies, were used: a) to purchase illicit goods and services such as drugs, credit card information, personally identifiable information, child pornography, and a range of criminal services; and, b) to launder illicit proceeds particularly as a means of facilitating overseas money transfers.

More recently, the growing use of decentralized digital currencies such as Bitcoin has enabled additional criminal activities. These include: Cryptojacking, which is the use of malware or compromised websites to hijack the computing power of others to obtain cryptocurrencies through mining; the theft of crypto assets directly, generally by targeting the private encryption keys of users; ransomware in which digital currencies are demanded as part of an extortion scheme; and attacks on the blockchain networks themselves.

As these decentralized currencies proliferate and evolve, new risks are emerging. Criminals are increasingly leveraging anonymity-enhanced currencies and services such as cryptocurrency tumblers and mixers to obscure transactions on the blockchain. In order to counter all these diverse illicit activities, effective law enforcement requires robust cooperation, both domestically and internationally, between law enforcement and regulatory agencies as well as thoughtful partnerships with industry.

Consequently, the Secret Service remains squarely focused on hiring, developing, and retaining a skilled and experienced investigative workforce. We are committed to working with partners across the law enforcement community to jointly train and develop shared technical solutions. The constant development of investigative capabilities is how we maintain our ability to effectively respond to innovations of technology now and into the future. Lastly, continued attention is needed to ensure that law enforcement agencies maintain lawful access to critical sources of evidence regardless of where or in what form that information is stored.

In closing, let me speak directly to those who seek to further the illicit activities through the use of digital currencies. As the investigative work of the United States Secret Service and our law enforcement partners continues to demonstrate, we are relentless in enforcing the law, and we will not be stopped by the perceived anonymity of digital currencies or the broader Internet.

Thank you again for your opportunity to testify and I look forward to your questions.

[The prepared statement of Mr. Novy can be found on page 41 of the Appendix.]

Chairman PEARCE. Thank you.

Mr. Ott, we have introduced you previously and I recognize that your just in time manufacturing has walked in just in time. If you are settled, we will recognize you for 5 minutes.

STATEMENT OF THOMAS OTT

Mr. OTT. Chairman Pearce, Ranking Member Perlmutter, and Members of the subcommittee, thank you for inviting me to speak today on behalf of the Financial Crimes Enforcement Network commonly known as FinCEN.

FinCEN has a leading role in the regulation of virtual currency activity and supports law enforcement investigations involving virtual currency and related financial crimes. So, I appreciate the opportunity to discuss our work in this space and the national security implications and illicit finance risks presented by virtual currency. FinCEN also works to combat the threats presented by both traditional and emerging payment systems while promoting responsible technological innovation throughout the financial sector.

In 2011, FinCEN issued a regulation that defined money transmissions services as the acceptance and transmission of currency, funds, and other value that substitutes for currency by any means. The 2011 rule serves as the foundation of our regulation of certain virtual currency activity. In March 2013, FinCEN issued guidance to clarify that virtual currency exchangers and administrators generally qualify as money transmitters under the Bank Secrecy Act.

Virtual currency payments pose illicit financing risk and necessitate careful assessment and mitigation. In particular, we are concerned about the growing use of decentralized convertible virtual currency to facilitate cybercrime, fraud, extortion, drug trafficking, money laundering, and other transnational crimes. FinCEN estimates that at least 4 billion in virtual currency has moved through the dark Net marketplaces since 2011. While traditional financial methods remain the primary vehicle for illicit activity, FinCEN believes virtual currency presents specific illicit finance risks and that without vigilance and targeted action, the scale of this activity could grow.

FinCEN has increasingly prioritized identifying, tracing, and disrupting the flow of illicit virtual currency activity. To that end, FinCEN examines financial institutions for compliance with their regulatory obligations to prevent money laundering and terrorist financing. In 2014, FinCEN together with its delegated examiners at the IRS have conducted examinations at more than one-third of all registered virtual currency money transmitters in the United States.

FinCEN has also taken significant enforcement actions. In July 2017, acting in coordination with our law enforcement partners, FinCEN assessed a penalty of over $110 million against BTC-e, an Internet-based foreign located money transmitter for various BSA violations. As part of this action, FinCEN also assessed a $12 million penalty against one of BTC-e's operators, the highest penalty we have ever assessed against an individual.

Collaboration is critical to combat the growing threats presented by virtual currency. Just last month, I met with my enforcement counterparts at the CFTC (Commodity Futures Trading Commission) and the SEC. My staff and others at FinCEN carefully and closely coordinate with these agencies on an ongoing basis.

One area where we continue to work together is on the illicit finance risk surrounding the recent growth of the initial coin offerings or ICOs. While ICO arrangements vary and, depending on their structure, may be subject to different authorities, one fact remains clear: FinCEN along with our partners at the SEC and CFTC expect businesses involved in ICOs to meet all of their AML (anti-money laundering) CFT (combating the financing of terrorism) obligations.

As both a former police officer and a former Federal prosecutor, I also want to highlight the important collaborations FinCEN has with our partners in law enforcement. FinCEN has provided support in over 100 cases since 2016. FinCEN's experts trace different types of virtual currency activities, identify suspicious sources of funds, target unregistered MSBs that do business in whole or in substantial part within the United States, and help disrupt transnational criminal networks operating in virtual currency.

Foremost, among our challenges in combating this activity, is the lack of consistent AML CFT regulations and supervision of virtual currency activity in most jurisdictions around the world. FinCEN and other Treasury components are working with the Financial Action Task Force or FATF and the Egmont Group to engage key jurisdictions directly to address these vulnerabilities. FinCEN looks forward to working with the committee, the law enforcement partners, the public sector, and our regulatory partners to identify strategies to help the United States remain both a global hub for innovation and a safe and secure financial system.

Thank you again for having me here today. I am happy to answer any of the questions you may have.

[The prepared statement of Mr. Ott can be found on page 48 of the Appendix.]

Chairman PEARCE. Thank you, Mr. Ott.

I now recognize myself for 5 minutes for questions. Mr. Novy, you quote on page four of your document about the different cryptocurrencies, the different exchanges that exist, how do you—many times these are very dark—how do you go about establishing those? How easy is it to find out about them?

Mr. NOVY. Thank you, Mr. Chairman. So, in the Secret Service when we conduct our investigations, we target any and all technologies or currencies that can be used for illicit activity. And so, therefore, digital currencies or virtual currencies are one of those types of technologies or means of transacting. So, what we do is in our undercover operations or through our operations in our criminal investigations, we investigate and look for different currencies, different transactions, different ways that crimes are committed and then we look to see how they are doing it.

We also do that through criminal informants. Criminal informants introduce us to those different areas as well. And so, that is how we learn these things.

Chairman PEARCE. I guess my question is, do you know what you don't know? Do you know how many currencies are out there that have not yet surfaced? Do you have a good feeling for that and how do you go about identifying them?

Mr. NOVY. That is a very good question, Mr. Chairman. The answer is we have an understanding that there are a lot of digital currencies out there. We don't know every single one of them. We understand a majority of the major ones, but currencies and coins can be created through technology. So, we don't know every single one of them. But through our partners of our Electronic Crimes Task Forces, which are both members of academia, of the private sector as well as other law enforcement, we collaborate together to learn and teach each other what each of us learns and that is how we keep up with it.

But the answer is I couldn't tell you how many digital currencies or virtual currencies are out there, but as they come up and they are used by—

Chairman PEARCE. Yes, sure. You also quote fairly significant numbers of transactions and are you pretty comfortable that those are accurate?

Mr. Ott, let me ask you that because I think, don't you have an intersection of responsibility right here at this point, aren't you both looking at the same issues?

Mr. OTT. Yes, Chairman. We have, through our intelligence division, we regularly track the incoming BSA filings, analyze those based on our business rules and be able to analyze that, put together a piece that would disseminate that to—

Chairman PEARCE. Are you pretty comfortable that you know what is going on?

Mr. OTT. The financial institutions are a very great partner and the best resource for that type of information. Yes, sir.

Chairman PEARCE. I guess one of my deeper concerns is—well, let me switch over to a different question. Not all the transactions are illicit with the digital currency. Is that correct?

Mr. OTT. That is correct.

Chairman PEARCE. And so, if digital currencies are used for legitimate transactions, how does say the IRS identify tax liabilities for legitimate operations if you have a digital currency?

Mr. OTT. Well, again, that would be—I am not familiar with the IRS procedures as it responds to virtual currency. FinCEN focuses on money transmissions. I know that we certainly work very closely with all law enforcement agencies as well as—

Chairman PEARCE. OK. If I could interrupt, I am running out of time here. I want to drill down on this a bit. If any of you have an idea because this to me is one of the biggest exposures that we have is legitimate goods and services being bought by very difficult-to-track transaction methods, and, at some point, you undermine the entire stability of society because society does work with its safety nets, with government spending off of taxation.

And if that becomes more difficult to pursue, if it is more difficult to identify what those transactions are, then, I am just wondering is anybody thinking about this aspect, maybe right now the digital currencies are not that prevalent, but in a matter of time, they will

be unless we understand what we are dealing with. So, if somebody wants to wrap up in a 30-second answer here.

Mr. NEVANO. Chairman, I will take that question. It is my understanding that the IRS treats virtual currency as property and therefore, the sale of virtual currency actually is subject to capital gains tax.

Chairman PEARCE. OK. But that is assuming they can see it. And all of you are talking in your testimony about many of them are invisible. And so, how are they going to identify it as a property if it is not too visible. That is my question and I will leave it dangling in the air here.

We go to Mr. Foster now for 5 minutes.

Mr. FOSTER. Thank you, Mr. Chairman.

Deputy Assistant Director Nevano, are you aware of any higher-ranking ICE officials who will be testifying before Congress who might address the crisis being caused by this Administration's polices of children being deliberately separated from their parents?

Mr. NEVANO. Congressman, at this time, I am not aware of any—

Mr. FOSTER. So, you are all we have. OK.

Now, first on the issue of family separation, I understand the Administration has announced plans to expand its capacity for holding children who have been separated from their parents in facilities sometimes known as "baby jails". And I was wondering if you can give this committee any further information about what this expanded capacity will look like. Specifically, will ICE be constructing more cages to separate children from their parents? Will this expanded capacity be in the same location as the children's parents where they are being held or elsewhere?

And what sort of childcare training are the personnel running these facilities being given? And are the background checks for these personnel up to the standards that we expect for childcare in the United States?

Mr. NEVANO. Chairman, thank you for your—Congressman, thank you for your question. I am here to testify today regarding virtual currency. I work for the director within the Department of Homeland Security. That is Homeland Security Investigations and our mission is basically to combat transnational criminal organizations that seek to basically exploit our immigration customs laws.

I do not work for the director within the Department of Homeland Security that handles the matters that you have addressed. I would be happy to take your questions back and have someone appropriately answer those questions, but that would not be me sitting in my position with Homeland Security Investigations.

Mr. FOSTER. Yes. So, I will be submitting those for the record and look forward to your responses on them because this is just a crucial issue.

Now, more locally in my district, ICE in the last month or so has executed a number of raids. ICE conducted a 6-day enforcement action in and around my district. I was told from advocates on the ground, which were later confirmed by the Chicago Tribune and others, that ICE agents pulled over and detained one Victor Cortez, a Mexican national who is here legally, visiting a friend in Joliet, Illinois in my district. Mr. Cortez was in the country legally with

a valid visa and Mr. Cortez produced this visa for ICE agents and yet despite this, he was still detained for several hours.

And so, my first question is, is it a common practice for ICE to pull over and detain anyone simply because they look Hispanic or speak with an accent?

Mr. NEVANO. Again, Congressman, I appreciate your concerns and your questions. I am not familiar with the situation that you are describing. Again, I work for the Homeland Security Investigations Directorate and that does not sound like something that HSI would have been involved in. I am happy to take the questions back for the record and provide you the answers that you require, sir.

Mr. FOSTER. OK. So, this issue of pulling people over where they actually—there is an illegal—they are here legally and are being pulled over, it is a little bit personal to me. My wife is an immigrant from Korea, but here obviously legally. Can she expect also to be pulled over because someone thinks that she doesn't look like an American?

Mr. NEVANO. Again, Congressman, I am not familiar with the situation. I will tell you that all HSI agents go through specific training, are trained not to profile and to conduct targeted law enforcement investigations. Again, specific circumstances you are talking about, I am not prepared to testify here today with those circumstances, but I would be happy to take those questions back and provide you a response.

Mr. FOSTER. Yes. I would be interested specifically on the profiling of Mr. Cortez. Is it a common practice for ICE to impersonate police officers and conduct traffic stops or is that part of your training as standard operating procedure?

Mr. NEVANO. Well, ICE deportation officers as well as special agents are considered, in our view, police officers. We are law enforcement officers, but to deal with the specific questions that you are talking about, I don't know the specifics. So, it is hard for me to provide you an answer without knowing those specifics. Again, I am happy to take those questions back and respond appropriately once those questions are submitted for the record.

Mr. FOSTER. Thank you. And I also think all of Congress looks forward to your superiors having the courage to appear before Congress to answer for the outrage that is happening in our southern border. Thank you.

Chairman PEARCE. The gentleman yields back.

And the Chair would now recognize the gentleman from North Carolina, Mr. Pittenger, for 5 minutes.

Mr. PITTENGER. Thank you, Mr. Chairman.

Again, thank each of you for your statements today and your insights on these critical issues. I would ask you in these illicit cases that you have identified, are the perpetrators that you have previously flagged, are they suspicious? Are they regarded as being engaged in other activities outside of cryptocurrency, or is this a traditional group of people, the same plot of actors or is this a new breed?

Mr. NOVY. Congressman, I could take that. So, a majority of the cyber criminals that we go after, a majority of them are using some type of virtual currency to move their money, to launder their

money, to either make sales or purchases of illicit items or to further their crimes. We are actually going after the criminals. And then, as we are going after the criminals, we come across the ways that they are moving money and the ways that they are laundering money.

And so, as Secret Service agents, we are financial crimes investigators as we have been since 1865, and so, like I said in my testimony, we follow the money.

Mr. PITTENGER. So, these are traditional criminals that have been involved in previous criminality.

Mr. NOVY. They could be. They could be. But the thing is, sir, they are pretty sophisticated these days. These days, the cyber criminals of today are a little bit different than the bank robbers of yesterday, but they are still doing the same thing, trying to steal the money.

Mr. PITTENGER. Yes, sir. There is also evidence suggesting that cryptocurrencies are increasingly used in money laundering schemes by organized criminal groups. But does U.S. law enforcement see any trends in the use of cryptocurrencies for money laundering related to drug traffickers, human traffickers, or the trade-based money laundering?

Mr. NEVANO. As my colleague from the Secret Service stated, we investigate all crimes, all crimes in the dark Net. So, yes, we would be concerned with drug traffickers, human traffickers, all individuals who are involved in nefarious activity. I think the goal of using these cryptocurrencies is the anonymity that they believe it provides.

So, we in law enforcement obviously face challenges at times to determine who they are. Some of these individuals still use traditional means such as third-party money laundering, trade-based money laundering. But those who want to be pseudo-anonymous actually use these decentralized cryptocurrencies to conduct their businesses on the dark Net.

Mr. PITTENGER. Do we have any estimates in terms of percentage, the amount of these crimes that are conducted cyber or otherwise with just the illicit use of cryptocurrencies? How much of a factor is it?

Mr. NOVY. Congressman, I can't come up with an exact percentage right now, but I can tell you that a good majority of the crimes that the Secret Service investigates, virtual currencies are used in those transactions, primarily because when they are transacting online in the dark Web or using criminal forums, that is how they can easily move money without having to talk to each other or communicate but also use anonymity.

Mr. PITTENGER. Do you have the legal latitude to perform your duties? Are there any legislative interests that you have that will give you greater capability to be successful in your duties in stopping illicit finance?

Mr. NOVY. For the Secret Service, I think I am not comfortable with the Secret Service suggesting that, but I will tell you that as technology increases, we use the laws and authorities that we have today. But, with that being said, we always have to look to see what is going to be the next crime, what is going to be the next step.

And so, we would say that we are always looking to make sure that laws and statutes are always kept up-to-date so that we can maintain and keep active what we can get.

Mr. PITTENGER. Is there anything that you see now, are there any impediments now legally that impede your ability to perform?

Mr. NOVY. I would say currently—currently, I would say the CLOUD Act was a very good step in moving forward for us to be able to get access to evidence, digital evidence in such an area. I would say as we use that and as we move forward, I would look to make sure that we still maintain access to lawful access to digital evidence that we can get from—when we serve subpoenas and court orders.

Mr. PITTENGER. Yes, sir. Anybody else want to comment on that point?

Well, my last question would be related to just—do you believe that there are additional factors that would limit terrorist exploitation of virtual currencies and how could they impact the domestic or international counterterrorism community focus on this front?

Mr. NEVANO. I think as we stated, all transnational criminal organizations, people involved in nefarious activities, there is obviously a desire to be anonymous and the use of cryptocurrencies would be one. So, I think it is definitely a possibility that we all need to be concerned about.

Mr. PITTENGER. Yes, sir. Thank you. My time is expired.

Chairman PEARCE. The gentleman's time is expired.

The Chair would now recognize the Ranking Member of the full committee, Ms. Waters, for 5 minutes.

Ms. WATERS. Thank you very much.

Mr. Nevano, I know that you are here to testify about the illicit use of virtual currency, but that is only one aspect of your job. As I see it, you are responsible—you are the Deputy Assistant Director responsible for the Illicit Trade, Travel, and Finance Division of Homeland Security Investigations and U.S. Immigration and Customs Enforcement. Is that right?

Mr. NEVANO. That is correct.

Ms. WATERS. OK. Can you tell me what you do with that aspect of your job that is described as U.S. Immigration and Customs Enforcement?

Mr. NEVANO. So, I work for the Department of Homeland Security which Immigration and Customs Enforcement is a directorate under the Department of Homeland Security. Within Immigration and Customs Enforcement, there are several components: Homeland Security Investigations being one, Enforcement Removal Operations being another. I do not work for Enforcement Removal Operations. I work for the criminal investigations side, which is Homeland Security Investigations.

Ms. WATERS. Are you familiar with the zero tolerance policy of the agency?

Mr. NEVANO. Yes. I have heard of it. I know it is all over the news.

Ms. WATERS. Well, I need you to help me understand a few things. If a mother and child or children go to what is known as a port of entry to claim amnesty, do you have anything to do with

that at all or your department, under Immigration and Customs Enforcement, have anything to do with that aspect of the agency?

Mr. NEVANO. So, if an individual shows up at a port of entry and claims asylum, they would be dealt with by our Customs and Border Patrol, which is basically under the Department of Homeland Security. How my directorate would be involved in individuals who are claiming asylum is more from the fraud standpoint. If there were facilitators who are actually organizing frivolous claims of asylum here in the United States, it would be my directorate that would actually look into those frivolous claims, but we are not the frontline who are dealing with these individuals when they come—

Ms. WATERS. So, explain to me how it works. So, a mother and children show up at the port of entry claiming amnesty and as I understand zero tolerance policy, they are not facilitated in the way that we thought the law works. They could be subject to detention at that point. What happens to the child at that point?

Mr. NEVANO. Again, Congressman, I am not familiar with the current practices along the border because I do not work for that directorate. So, I cannot comment, but I would be happy to take those questions back for the record.

Ms. WATERS. You are the Deputy Assistant Director and U.S. Immigration and Customs Enforcement is part of your responsibility or oversight. Do you supervise anybody in that division?

Mr. NEVANO. So, again, I do work for Immigration and Customs Enforcement, but specifically for Homeland Security Investigations and we do not have people on the frontline who are making those determinations of admissibility when an individual enters the United States.

Ms. WATERS. What and how do you investigate someone who is claiming amnesty who is thought not to be eligible for amnesty? What happens to them at that point?

Mr. NEVANO. We don't investigate every single person who claims—

Ms. WATERS. But the ones that you do investigate, what happens? How do you do that?

Mr. NEVANO. We are looking more to the facilitators, the organizations who are exploiting these individuals who are claiming asylum, taking their money, filing frivolous claims. That is more what Homeland Security Investigations does. We are not looking at every single person who files an application.

Ms. WATERS. I know that you may not be looking at every single individual, but those that you do look at, maybe it is a mother with children who you think may be part of a ring where they are trying to get folks into the United States at the port of entry, you have to investigate them. You don't investigate all of them, but when you do, how does it work?

What do you do from that point? And if you want to continue the investigation because you are suspicious, you have enough information that would lead you to believe that something is going on, what happens to the child? Who has the responsibility for taking the child if you are going to retain the woman or the family? What happens at that point?

Mr. NEVANO. Again, Congressman, I do not deal with the detention of individuals. Those decisions are made by another direc-

torate. We are on the backend. We are investigating when people have already made an entry into the United States. They may have a hearing before an immigration judge here in the United States. We are not involved in that.

Ms. WATERS. So, you are not involved in the supervision of that aspect of your job at all. Is that right?

Mr. NEVANO. That is correct.

Ms. WATERS. Thank you very much. I yield back the balance of my time.

Chairman PEARCE. The gentlelady yields back.

The Chair now recognizes the main man from Maine, Mr. Poliquin, for 5 minutes.

Mr. POLIQUIN. Thank you very much, Mr. Chairman. Thank you, gentlemen, for being here very much. I appreciate it.

You folks deal with criminal activity at the Federal level or from a Federal standpoint and you have a lot of tools available to you that we don't have up in Bangor, Maine or Lewiston, Maine, both of which I represent. I represent the rural part of Maine and Bangor and Lewiston are part of my district.

Tell me a little bit about the type of training that you folks might extend to law enforcement officials on the ground at the local level in our great State and other parts of our country. Mr. Nevano, who wants to take a shot at that?

Mr. NOVY. I will take that one.

Mr. POLIQUIN. Yes.

Mr. NOVY. So, the Secret Service, we actually have partnered with the State of Alabama and we have the National Computer Forensics Institute in Alabama.

Mr. POLIQUIN. Right.

Mr. NOVY. Fantastic operation, fantastic organization and what we do there is we train solely State and local law enforcement, prosecutors, and judges. The Secret Service, we focus on the law enforcement portion of it while the State of Alabama District Attorney Association focuses on the prosecutors and judges.

And what we do is we take the same level of training that we give our Secret Service agents and we provide that to State and locals especially for someone like your folks in Maine, upstate, downstate, wherever you are going to go. The idea is we are looking to train the cyber supply chain if you want to call it, all the way from law enforcement all the way up to judges so that they completely understand and we don't leave them alone.

The main thing is after they get their training, they actually leave with the equipment that they are trained on because many times, they can't afford a digital forensic lab of their own. So, when they leave there, whatever equipment they are trained on, they actually get that equipment. They take it back to their police department and use that at their police department to work on any investigation. It doesn't have to be a cyber crime. It could be a rape. It could be a murder. It could be a bank robbery. It could be any type of crime.

The main thing, though, is when it deals with cyber, cyber is really difficult technology and sometimes it takes a little bit more. And so, we don't leave people hanging out there as well. What we do is we connect them to our electronic crimes task forces. By doing

that, let us say an officer in Maine has a hard time trying to figure out a forensic tool or something along those lines, we will work with them through our Electronic Crimes Task Force primarily in Boston, but we will actually send agents up to Maine if we need to, to help them understand. We will work whatever they need to work on.

Mr. POLIQUIN. My primary constitutional responsibility, Mr. Novy, is to protect our families and there is no one who is more pro jobs, pro business, pro national security, pro protecting our families than I am. So, I really appreciate you giving me that information because it is all hands on deck. We have to make sure that the folks at the local level who are the frontline, that thin blue line, have the tools they need to do all of this work. And this whole cryptocurrency and everything else is new to a lot of folks and very complicated.

Let me morph a little bit and maybe, Mr. Nevano, this would be for you, but if not, someone else jump in, ransomware where bad actors are able to put a virus or something else on your system whether it be personally or at a business and effectively contact you and say, "Unless you pay us X amount of money, we will let this virus run rampant and destroy your system and interrupt your workflow" and which could kill jobs and so forth and so on.

What about the use of cryptocurrency to pay that ransomware—excuse me, that ransom, if you will, to remove that problem from your network? Do you folks run into that and how in the heck do you fight that? How do our folks at the local level fight that?

Mr. NOVY. I will take that one as well, Congressman.

Mr. POLIQUIN. Thank you.

Mr. NOVY. So, ransomware, actually we believe at the Secret Service, has proliferated from the use of digital currencies because it is used in just about every payment that you can imagine for ransomware, and because of the anonymity and the quickness that you could make a transaction, that is why people use virtual currencies for ransomware.

The tough thing about ransomware is it does take preparation. People should take into consideration basic cybersecurity and basic cyber practices. People should have backups to their systems. In the Secret Service, we have actually gone out and done a whole bunch of workshops all around the Nation with us as well as with the Financial Services Information Sharing Analysis Center as well as the FBI where we have gone and we have taught different courses and classes of how to defeat or how to get prepared for ransomware.

But to answer your question, virtual currency has actually been the propagator for ransomware we believe.

Mr. POLIQUIN. If I call Bill O'Malley who is the Chief of Police in Bangor or Phil Kroll who is the Chief of Police in Auburn, Maine, would they know who to call at your shop to get help for any of these issues? Are you folks pretty good as far as outreach to our local folks in the ground?

Mr. NOVY. Yes, absolutely. So, we have an office in Portland, Maine and that office in Portland, Maine is actually there to go and liaison with all law enforcement agencies no matter how big or small they are in your State.

Mr. POLIQUIN. OK.

Yes, sir.

Mr. NEVANO. I am familiar with your AOR being from New England and I know that we have multiple task forces. We have an office in Portland, Maine; Bangor, Maine; as well as Houlton, Maine. And I know that we have several task forces in those areas where we work every day and collaborate with State and local law enforcement officers in your district.

Mr. POLIQUIN. Great. Well, thank you very much, and I do want to—

Chairman PEARCE. The gentleman's time is expired.

Mr. POLIQUIN. How do you divide your loyalties between the Red Sox and the Nationals if you are from New England? It is not easy.

Thank you, Mr. Chairman. I yield back my time. The witness does not have to answer that question.

Chairman PEARCE. It was not the lapse of time. It was your problem with the last statement. Thank you.

But now, I recognize the gentlelady from New York, Mrs. Maloney, for 5 minutes.

Mrs. MALONEY. Thank you. I thank the Chairman for yielding.

Mr. Nevano, first of all, I would like to thank all of the panelists for being here. But, Mr. Nevano, I am sure you are aware of what is happening at our southern border. Children including babies are being ripped out of their parents' arms and these people were just merely looking for a better life for their families here in the United States. It is nothing short of government-sanctioned child abuse and runs counter to everything that we stand for as a Nation.

I have seen photos of children in cages, heard recordings of children crying, and spoken with fathers at a detention center this past weekend in New Jersey where they came legally seeking asylum and were put into detention prisons. And one father said, at three o'clock in the morning, they came and tore his daughter from his arms. And just last night, the Associated Press reported that babies and toddlers are being shipped literally hundreds of miles away from their parents to be housed in so-called tender age facilities.

Make no mistake. I don't care what they are called. These are prisons—prisons for babies. And has this Administration no soul? Have they no basic human empathy? This is not governance. This is not enforcing existing law. This is law that was made up by this Administration. And it is stone cold evil and is entirely the choice of this Administration and a reflection of a heartless ideology.

So, my question, Mr. Nevano, is that surely many ICE agents are mothers and fathers in addition to their role with the agency. Is there any concern among your colleagues about the irreparable damage this policy of separation will have on these children?

Mr. NEVANO. Congressman, thank you for your question. Again, working for Homeland Security Investigations, we are not involved in that aspect of what you are speaking about. I am a parent and of course I understand exactly what you are saying. I have been doing this job for 27 years. I am a law enforcement officer and I certainly understand what you are saying.

But I am not here to comment on that because I am here to testify on virtual currency. I would be happy to take any specific questions you have back for the record.

Mrs. MALONEY. Well, this Administration has deliberately chosen this path and would you agree that the Administration has the authority to change this policy? But now I know you are not going to answer, but I do believe they could change it.

But before I close, I would like to play a very troubling recording that has been widely circulated in the news this week.

[Audio recording played.]

Mrs. MALONEY. Well, I just want to close by saying as a mother of two children, I find this policy absolutely unconscionable. I cannot imagine what it is like to have your children torn from your arms and these are people that are just seeking a better life for their families. They are coming here seeking asylum. We have always been a beacon of hope to the world, and persecuting and separating children from their families is just un-American and just plain wrong.

And it is an outrageous policy. It needs to end and we need to make sure the Administration absolutely never does it again. I thank you very much and I yield back.

Chairman PEARCE. The gentlelady yields back.

The Chair would now recognize the gentleman from Ohio, Mr. Davidson, for 5 minutes.

Mr. DAVIDSON. Thank you, Mr. Chairman, and thank you to our witnesses, I appreciate your expertise on financial crimes enforcement, illicit finance, and particularly related to cryptocurrencies today. Hopefully, we can stay on topic during my 5 minutes, I will try to stay focused on the topic at hand. Because it is hard to get these hearings scheduled, so thank you, we can't change course on hearings all the time because of the news of the day, pressing as it is, I trust that we are on a path to a better policy in all sorts of arenas, including this one which we are here to work on.

So, the past several years I have been watching the growth of digital assets and cryptocurrencies and I am excited about the opportunities they create. And I am curious just in terms of framing this issue, it is very important that your tools in your kit bag stay in compliance with current laws. And we have illicit finance denominated in U.S. dollars, correct? Correct?

Mr. NOVY. So, Congressman, it could be denominated in a number of things, the cost or the value of digital currency—

Mr. DAVIDSON. No, no. I am not talking about cryptocurrencies, I am just—the cash, cash in bags, duffel bags of cash, hay bales full of cash, ship containers full of cash, rail cars full of cash, suitcases full of cash, we transact in cash, right?

There is also illicit finance in hawala networks, right? These things aren't illegal, we are looking for ways to be able to—U.S. dollars aren't illegal, carrying cash in a satchel is not illegal. Though we have set trip wires in place like crossing a border with too much cash without reporting that they are crossing a border with too much cash. These are the things that help you catch that.

Still struggling last I heard about hawala networks and things like that. Though operating a hawala network isn't illegal, operating one to do illicit things is. And I guess, how do we apply those

sort of kit bag things to cryptocurrencies so that we protect the use of cryptocurrencies, yet have the trip wires that help us detect illegal activity with the cryptocurrencies?

Mr. NEVANO. So, when we conduct our investigations, as you are mentioning all tools in our tool bag are used, whether it is traditional schemes to attack money laundering, which would be as you are mentioning: Bulk cash smuggling, third-party money laundering, trade-based money laundering, we also—as my colleague from Secret Service mentioned, use of confidential informants, use of undercover operations, whatever we can do to basically detect, disrupt, and dismantle those organizations, whether they are using the traditional methods that you are speaking about, or cryptocurrencies, we are trained to actually attack the problem as it exists.

Mr. DAVIDSON. In general, when something moves across an electronic format, is it easier to have record keeping on that than say hawala or cash? Even cryptocurrencies? There is a record, right? A searchable record or queriable record?

Mr. NOVY. So, Congressman, the answer is usually yes. Usually when it creates a record there is an electronic record that can be followed. However, in virtual currencies sometimes it can be obscured through tumblers or mixers, or something along those lines as well. So, there is a record if you can find it, but sometimes it is a little bit harder to find.

Mr. DAVIDSON. OK. And so, additional guidance has been given to provide compliance as money service businesses for people that are doing these transactions in the U.S. We have places that don't comply with those laws just like we have it for people who don't comply with it for wires and other ways that we do it with cash.

I am concerned about, in the States, we have all sorts of regs that are duplicative. Wyoming has some laws related to crypto, but so does New York. I am not sure why New York needs such a heavy-handed AML provision, do you view the duplication as counterproductive, would it be easier to have a uniform reg across the country or is it easier to have State-based systems as well?

Mr. OTT. Well, Congressman, for FinCEN's perspective, of course we are on the Federal level, but many we recognize that we work very closely with some of our State regulators as well, they adopt many of the similar provisions as are found in the Bank Secrecy Act, and what we find in terms of the biggest challenge that we have in regulating virtual currency is in fact, an inconsistent or lack of consistent AML CFT regulations internationally that open up vulnerabilities within the United States. And I believe, while we are working with our foreign counterparts to try to correct that situation, feel that there will still be a vulnerability until we have that international cooperation.

Mr. DAVIDSON. Thank you, my time has expired.

Chairman PEARCE. The gentleman's time is expired, the Chair will now recognize Mr. Vargas for 5 minutes.

Mr. VARGAS. Thank you very much, Mr. Chairman, I appreciate the opportunity. Again, I want to thank the three witnesses here today, as I especially want to thank them for your diligent work against illicit use of cryptocurrency, especially in sex trafficking and drug trafficking. Again, thank you very much. I do, however,

want to ask some questions to Mr. Nevano, I am taking a look here at the information that you sent to us and it does say, U.S. Immigration and Customs Enforcement right at the top.

And I think when you were introduced, we heard that you had more experience than your present job. Could you repeat again, your career has been long, it has been 27 years in law enforcement and we appreciate that, what other experiences, what other jobs did you have with ICE?

Mr. NEVANO. Congressman, I started my career as an immigration inspector. That is where I started my career. I became a special agent. I worked my way up to be a group supervisor. Assistant special agent in charge. As you are probably aware, in 2003, Immigration Naturalization Service and Customs actually merged to form Immigration and Customs Enforcement, Homeland Security Investigations. Since my time in headquarters, I have worked as a unit chief in asset forfeiture, I was the chief of staff for the deputy director of Immigration and Customs Enforcement. And I was also now in my position, I am the Deputy Assistant Director for Illicit Trade, Travel, and Finance.

Mr. VARGAS. So, you do have quite a bit of experience beyond simply working in the position that you have today, I think some of the questions that we were asking of you were questions maybe that you do have some experience on. I do want to ask some myself, are you familiar with the family—the Family Case Management program?

Mr. NEVANO. I have heard of it, sir. I know it is part of the enforcement removal operations portfolio; I am not intimately, though, knowledgeable about it.

Mr. VARGAS. OK. It had an almost 100 percent court appearance rate, so this is where the families were not separated instead they were able to stay together, and then they had to come back for court appearances, it almost had a 100 percent rate of people coming back for their court appearance, it was very, very successful.

It didn't—they did this for families that weren't flight risks and they weren't dangerous, it was quite successful, I don't know why we stopped it. But that is one of the reasons why there has to be the separation of families the President says, there does not have to be, when, in fact, the President claims the DHS is required to separate families under current law, I don't understand, maybe you could explain that to me.

Contrary to claims by the Attorney General, the Bible in Romans 13, which I know well, I studied to be a priest for a number of years, it is not statutory authority. It doesn't justify this horrific and unconscionable policy. But can you point to any statutory authority mandating that families be separated because, I can point you to these—the Family Case Manager program that didn't do this, didn't separate the families?

Mr. NEVANO. I am not familiar with any statutes that require that, Congressman.

Mr. VARGAS. I can tell you this and I think you would agree with this, I represent the border in California, and I do go and visit not only with ICE but the CBP and BP, Border Patrol, I can tell you this what they are doing today, your agents, they are bringing diapers that they are paying for themselves, milk for kids, other

things that these children need, because they know they are going to be separated, and they think because like you, they are parents, they think they need these things.

If you ask your own agents out there, you will tell—they will tell you, they do not like what they are doing, they are not happy about it, they are spending their own money trying to help these kids, are you familiar with any of that?

Mr. NEVANO. Congressman, again, I think you are speaking about Border Patrol agents—

Mr. VARGAS. No, no. I am also speaking about the CBP, and I am also speaking about ICE.

Mr. NEVANO. CBP is not under my directorate, so again, our special agents more than likely, unless they are investigating some type of transnational criminal organization entering the border, would not be involved in some of the circumstances you are speaking about.

Mr. VARGAS. But I think you are being very technical, because you do have experience within all of the range there, if you—as you would under—as you described to me earlier, you were in fact the line officer, you did in fact have—

So, what I would tell you is this, this policy that you have now, I wish you would go back and look at those and talk to your agents on the look—on the ground, they don't like it, they know it is not their values. When you go and you see like I had the opportunity to see on Monday these children, they just want their moms, they just want their dads. What we are doing is wrong. Certainly not based on Christianity or any type of religion that I am aware of, and it has to be reversed.

Your own agents, if you talk to them, they will tell you, and you can go there and see the diapers that they buy, the food that they buy for these children, because they are concerned about their own safety, the safety and the wellbeing of these kids when they are separated from their moms, they are parents too. If you would like to answer the questions.

Mr. NEVANO. Congressman, in my 27 years career, I have worked under several different Administrations, and during those Administrations with the change, laws continually change, the way we are enforcing laws. And, again, what you are speaking about now in the current environment I am not involved with what you are speaking about. We are involved in the aftermath, if there are individuals who are being so exploited, who are victims who are being supported by organizations, that is where we will come in to try to look at the facilitate—the people who are facilitating this activity.

Mr. VARGAS. Thank you, I yield back. Thank you.

Chairman PEARCE. The gentleman's time has expired. The Chair would now recognize Mr. Budd for 5 minutes.

Mr. BUDD. Thank you, Mr. Chairman. And again, thanks to the witnesses for your time today, for your expertise, all you do for security for our country. And I want to shift a bit to the topic, the original topic at hand, terror financing and virtual currencies. So, the Foundation for Defense of Democracies or FDD, they have been a great resource to me and staff on issues like this. And they recently reported the first publicly verifiable instance of an online propaganda unit, it was based in Gaza, in the Gaza Strip, calling

for Muslims worldwide to donate funds for terrorist purposes. They only raised a few hundred dollars, but even this is an early sign, I am thinking, and it is disturbing that terrorist financing mechanisms are evolving using this technology.

I have also seen evidence of Hamas groups embracing the technology and promoting Wallet apps like Telegram. So the question is, what is the likelihood that we see more propaganda or terrorist campaigns from groups like this in the future? And what can be done to prevent it from happening?

Mr. NEVANO. I am familiar with the article that you mentioned and I would agree with you that I believe there were only two individuals that actually volunteered to donate, it was somewhere in the vicinity of $500 that was—that was received, so although it was a low turnout as far as volunteers, it did something that law enforcement would be concerned about, because as virtual currency continues to grow, it is certainly an avenue that could be used for those types of propaganda situations to collect money in support of terrorist organizations.

Mr. BUDD. So even at a few hundred dollars, we still shouldn't dismiss something like this?

Mr. NEVANO. Absolutely not.

Mr. BUDD. OK. Thank you. Can you tell me what factors are limiting terrorist exploitation of the virtual currencies, basically what is working, and how that should impact the counterterrorism community, and Congress' focus on this front?

Mr. NEVANO. So one of the challenges I think is terrorist organizations are used to the traditional money laundering/bulk cash smuggling, hawala situations. I think one of the challenges that we may be facing for the traditional terrorist organizations that we are speaking about, is maybe some of the resources logistics, some of the locations that they are involved, and that they don't have the technology right now, but, over time with, as technology advances, et cetera, that certainly would be a concern.

In lone wolf terrorist type of situations where you may have a domestic terrorism situation, that, to me, would be a concern, because they would have the technology, they would have the access to the internet, et cetera, working right at home from their computers, and that certainly would be a concern.

Mr. BUDD. Thank you. Gentlemen, do you care to comment on what is working and how you would ask Congress to focus on this front?

Mr. NOVY. From the Secret Service standpoint, we are—our area is not terrorism or counterterrorism, but the—what we see is though, is that on the criminal side with the exploitation of digital currency to move forward their crimes, we know that terrorists look to gain education from how other criminals are doing things. And so, how other criminals are moving money, and then they can learn from that. So from my expertise, I see it going, as I see it rising in criminal activity, I would assume, that, at some point, the terrorists will start learning from the criminals.

Mr. BUDD. Good.

Mr. OTT. From FinCEN's perspective, I would just mention that we work very closely in partnership with the financial institutions in terms of our outreach and we see, have seen from 2016 to 2017,

a 90 percent increase in the BSA filings involving some type of cryptocurrency across the variety of criminal activities, whether that is terrorist financing, narcotics trafficking, money laundering, or other illicit activities. So to that extent, we are very pleased with the increase of the type of law enforcement intelligence that we can share with our counterparts.

Mr. BUDD. Thank you all for this, a little bit different type of a question, but I would like to get law enforcement's perspective on this, and it is a hot topic right now especially here in D.C. as we look at this as legislators, but how should we classify virtual currencies? Is it a security, is a commodity, another form of property? And what is the appropriate framework for us to use to work on legislation addressing virtual currencies?

Mr. OTT. Thank you, Congressman. I think—from again, from FinCEN's perspective, we certainly recognize that this is a complex area, we focus on money transmissions, specifically. So our concern is the transmission of either currency, finds, or what we say is a subset—of other value that substitutes for currency. And we have said that in our guidance and in our legislation that the current virtual currency is also included in that definition of other value, that substitutes for currency.

So we feel that certain regulatory regime right now, that we have in place, is sufficient to cover virtual currency, and to be—provide the correct reporting. And I would also say that that applies to whether or not an MSP or a money transmitter is located within the continental United States or outside the United States, but does substantial, either substantial business within the United States or other.

Mr. BUDD. My time has expired, I yield back.

Chairman PEARCE. The Chair would now recognize the gentleman from Georgia. Mr. Scott for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman. I am sitting here and I am absolutely amazed. You all are sitting here and just seemingly unknowledgeable about one of the greatest tragedies that we are faced with, with the treatment of these little children at the borders.

Now, Mr. Nevano, several Members have asked you, and questioned you, and reminded you that you do have responsibility here, you keep saying, you don't. Your entity deals with MS-13s, the gangs, the drug cartels, all of the very reasons that we got in this situation today. These people are putting their children first. I looked up there, I saw this picture of this little girl, I wish they would put it back up there at the truck and she is looking up, and you know what I saw from that?

I said what the Lord said, "Suffer the little children to come unto me: for of such is the kingdom of God." If you really understand that scripture is it because people were trying to push this one up to see, that one up, but He said no, it is the children who come first, that is why this Nation is crying out to stop this meanness.

There is the picture right there, look at it, Mr. Nevano, there it is right there, would you mind? That is the image of the United States of America, we have to stop it now. If you can't give information to us, you are the representatives of this Administration, that ain't the Democrats causing this, it is President Trump, and

take a message back to him. That the Lord said, "First, suffer the children to come unto me: for of such is the kingdom of God."

That is the scripture that they should be admonishing. Tell me, Mr. Nevano, when was the first tolerance, the zero tolerance policy first put into place?

Mr. NEVANO. Congressman, I am not specifically aware of when it was put in place, my recollection from hearing it in the news was maybe sometime around April.

Mr. SCOTT. How many children have been reunited since the zero policy has been put in place?

Mr. NEVANO. Again, I do not work in that directorate, so I do not have that information.

Mr. SCOTT. And you can see from the pictures there, that most have not been reunited. What is going to happen to these children? How many people who legally entered this country to seek asylum have been detained as a result of this policy?

Mr. NEVANO. Again, I do not have those numbers with me.

Mr. SCOTT. How many children separated from their families on the U.S.-Mexican border have had to enter the foster homes? The foster care as a result of this Administration's decision?

Mr. NEVANO. I do not have that information.

Mr. SCOTT. Yes. How many children may never see their mothers or their families again because of what this Administration has decided to do on the borders? Think about it.

I am telling you, man. We have to stop this. If there's any message to take back to the White House, tell them to stop it. This country has been blessed by God. Divine intervention is throughout our history, from the soldiers at Valley Forge, to those who went to Montezuma fighting. We are the beacon of hope, liberty, freedom of the world. The little girl on these pictures looking up, that ain't America. Please, will you take that message back to the President?

Chairman PEARCE. The gentleman's time has expired. The Chair would now recognize Mr. Crist for 5 minutes.

Mr. CRIST. Thank you, Mr. Chairman. I just have a few questions for you, Mr. Nevano. How many children have been separated from their families since the Trump Administration announced the zero tolerance policy on April 6, 2018?

Mr. NEVANO. I don't have that information. I am happy to take it back for the record, and see if our enforcement removal or our other component within DHS can get that information for you.

Mr. CRIST. Thank you. And I will provide these for you before you leave. What is the plan to reunite the children with their parents?

Mr. NEVANO. Again, I don't—I am not involved in the policy-making on that side of the enforcement house, I don't have that information, but, again, I am happy to take that back for the record.

Mr. CRIST. Physically, where is your office?

Mr. NEVANO. It is located at 12th & D Streets, sir.

Mr. CRIST. And your colleagues there, have you had any conversations about what is all over the news for the past 72 or so hours? Any concern about it?

Mr. NEVANO. I watch the news every morning like everyone else, and obviously see what is going on, but it is not a topic of conversa-

tion within my directorate, because, again, we are not involved in that activity.

Mr. CRIST. Nobody there has talked about this?

Mr. NEVANO. Absolutely, it is on the news, everyone is watching it, but it is not a conversation that I have. I was here to prepare for virtual currency and that is how I spent my past week or so preparing for this hearing on virtual currency.

Mr. CRIST. You have dedicated your life, it sounds like to appropriate law enforcement?

Mr. NEVANO. Twenty-seven years, I have.

Mr. CRIST. Do you think this is the right kind of law enforcement for the United States of America?

Mr. NEVANO. Again, I am not here to give my opinion, I am a sworn law enforcement officer, that I was sworn to defend the laws of the United States, but I am not here to comment on my personal situations, I am happy to take any questions you may have, but—

Mr. CRIST. I am not asking about your personal situation, I am just asking your opinion, sir.

Mr. NEVANO. I don't have an opinion on that, sir.

Mr. CRIST. OK, that is interesting. You have no opinion on this?

Mr. NEVANO. I have an opinion on what my job is and what I am required to do and—

Mr. CRIST. No, I am talking about what we are talking about.

Mr. NEVANO. Congressman, anyone who looks at that picture obviously would have concerns looking at that picture. I faced several of these situations in my career as an immigration inspector, and what I—what I have done is if I was directed to do something, I would do what the direction of the—my superiors in my Administration told me what to do.

Mr. CRIST. Even if you felt it was wrong?

Mr. NEVANO. That is my job, I swore on the oath to uphold the Constitution of the United States.

Mr. CRIST. But what if it is not a constitutional act they are asking you to do?

Mr. NEVANO. It may be a directive that we are following that is from our leadership, and that is what I do on a day-to-day basis, if I get direction from my leadership, I follow what my leadership's directives are.

Mr. CRIST. Follow right or wrong?

Mr. NEVANO. It is not my decision to make, Congressman.

Mr. CRIST. Yes, it is. Yes, you are a citizen of this country, you don't have to do everything you are told to do if you think it is wrong and immoral.

Mr. NEVANO. If there was something that was immorally correct or is not legal, then obviously I would not do that. But—

Mr. CRIST. I am glad to hear that.

Mr. NEVANO. Yes, absolutely. I have 27 years, and I have been doing my job for 27 years, I am a family member, obviously, situations like that when you see that, touch everyone's heart, but, again, we are not the ones to blame for this situation, meaning me as a special agent within my Homeland Security directorate, if laws need to be changed, they need to be changed, but it is not me to make the change in the law.

Mr. CRIST. I am not blaming you. I didn't say that. Who do you think is to blame for this?

Mr. NEVANO. I think obviously the laws need to be changed, I am not here to say who is responsible for it, but if the laws need to be changed, it is not for me as a deputy assistant director, at my level, to be making those changes.

Mr. CRIST. Do you know if any children have been physically harmed or died while in this custody since April?

Mr. NEVANO. That I am not sure about.

Mr. CRIST. Can you find out?

Mr. NEVANO. I am happy to take any questions you have and get it to the appropriate locations within the Department of Homeland Security.

Mr. CRIST. Thank you for your help.

Chairman PEARCE. The Chair would now recognize Mr. Heck for 5 minutes.

Mr. HECK. Thank you, Mr. Chairman, thanks to all the witnesses for being here today. I am not sure who can answer this question, anybody that has the answer I would appreciate. How long is the list of mothers with young children who have been detained at the border are suspected or known to have used cryptocurrency for illicit purposes?

Mr. NEVANO. I am not aware of that.

Mr. HECK. Any? So we can at least eliminate that category of reason to be afraid of young mothers with young children? Mr. Nevano, you have had a distinguished career, and I sincerely thank you for that at ICE. I would like to ask you if you believe that the current resources provided ICE and the staffing levels that result therefrom are 100 percent sufficient for the agency to fulfill its mission in a robust fashion?

Mr. NEVANO. Congressman, we have plus or minus 6,500 special agents within the Homeland Security Investigations, we could obviously use more—

Mr. HECK. No, sir. I asked about agency overall, drawing upon your 27 years, the question is very straightforward, does the agency overall, from where you sit, based on your 27 years of experience, have 100 percent of the resources and staffing it needs in order to fulfill its mission in a robust fashion?

Mr. NEVANO. Again, I am familiar with my directorate which is Homeland Security Investigations, I am not familiar with the other components within DHS, there are over 22 components within DHS, I am not familiar with every other component.

Mr. HECK. Is it your impression you have all the staffing and resources you need?

Mr. NEVANO. Within Homeland Security Investigations, we could certainly use more.

Mr. HECK. So, if that is also true, if the other divisions at ICE, we can reasonably and logically conclude that if they were asked to do anything additional, it would only come of the compromise or result in a compromise of their effort to fulfill their mission?

There is a Federal prison, Mr. Nevano, in Victorville, California where we now have about a thousand ICE detainees. Do you know whether or not the guards there have been trained to deal with the non-criminal occupants and immigrants at that facility?

Mr. NEVANO. No, I am not, Congressman, I am not aware.

Mr. HECK. Do you know whether or not the immigrant detainees are being accorded the same rights and privileges as the prisoners, violators of crimes, such as visitation and access to counsel and recreational opportunities?

Mr. NEVANO. I am not familiar with the situation in that facility.

Mr. HECK. I have a facility in my district that is called the Selma Carson Home which 16- and 17-year-old unaccompanied boys are kept, do you know if the current population includes anyone that has been separated from their parent?

Mr. NEVANO. I do not.

Mr. HECK. I guess I would like to make an observation if I may about this overall issue, because the truth of the matter is, I completely understand somebody that is deeply concerned about our Nation's security in general, and as it even relates to some degree with respect to borders.

What is difficult for me to understand is the obsession on just one border, and the obsession on only one fix to the issue there. I guess I can't forget the fact that a goodly number of the people who helped plot and implement the 9/11 attack on our soil, the deadliest in our Nation's history, came in through the northern border, not a lot of talk about enhanced northern border security. And I am very mindful of the fact that nearly 50 percent of the people who are here without the appropriate documents came in legally and just stayed.

And yet, all the focus seems to be on one of our four borders, the water on our east and west take care of that, nothing on the north for all practical purposes, nothing on the way the people who come here legally but stay.

I guess, in simpler terms, this strikes me as if somebody owned a home and they felt that they had a security risk of being robbed, they decide to build two walls, not four, two, in order to protect themselves, or even one wall, leaving the other two or three open. I guess that would be one way to try to protect themselves, not very effective, or they could buy an alarm system, or they could put up increase lighting, or they could trim the bushes that provide cover for people, or they could buy a dog, or, my point being, that the issue of security has to be solved intelligently. Not just with a half-baked, half idea on how to provide for our Nation's security. Thank you, Mr. Chairman, and I yield back.

Chairman PEARCE. The gentleman's time has expired. The Chair would now recognize Mr. Capuano for 5 minutes.

Mr. CAPUANO. Thank you, Mr. Chairman. Thank you gentlemen for being here. And honestly, I was looking forward to having a hearing on the subject matter that was advertised, but with today's crisis I assume by now you have figured out we just can't do that. We can't remain silent.

Mr. Nevano, I see you have an excellent education, I am a B.C. guy, too. My son as well. I don't remember being taught by any of the Jesuits it was OK to separate parents from children, and I want to be real clear, you have been incredibly professional under some tough questionings, and I respect your position, and I am not going to try to make you, put you in a tough position, because I think you have done a good job today defending the indefensible or

actually avoiding defending the indefensible. And I really do, I appreciate what you are doing, and I don't want to put you in a tough position.

But, you are the guy who is here, you are the guy we got, and I am sorry, but is there anybody behind you who can answer the questions that have been asked today? I don't know, something, anybody else from ICE who are here that can answer these questions?

Mr. NEVANO. I don't believe there is anybody with me here today from Customs and Border Protection Enforcement and Removal operations that may have some of those answers to your question.

Mr. CAPUANO. OK. I expected that. I know you have heard the audio before, but I want to play that audio just one more time, because I do have a question related to it. I don't know exactly all this technology stuff, but there's a guy in the backroom doing some magic, so.

[Audio recording played.]

Mr. CAPUANO. I think that's enough, I think that is all we need. I don't know. I appreciate it, thank you. Did you hear any MS-13 members in that audio?

Mr. NEVANO. I did not.

Mr. CAPUANO. I didn't either. Any other gang members that you could tell that secret code that we could tell that these children were somehow associated with an international gang that came here to terrorize us?

Mr. NEVANO. I did not.

Mr. CAPUANO. No, I didn't either. So, it was interesting that the President was able to hear that. I don't know, I know you have been testifying for a while, I don't know if you are caught up on the news, you probably not, but if you—it has been announced the President has just signed an order reversing his previous order. So, do you—I assume your agency is going to get some new orders.

But I am interested, I just heard the last 3 days, the President of the United States telling me repeatedly on the news, very publicly that he didn't have the authority to change his own zero tolerance policy, and now he has done it. Could you explain to me how the President could say on, for 3, 4, or 5 days in a row we didn't have the authority, and now somehow have the authority?

Is anybody at ICE going to ask questions as to who actually has the authority to make a determination whether children can be ripped from the arms of their mother?

Mr. NEVANO. I don't have that answer for you today, sir.

Mr. CAPUANO. No, I am just—I am just curious, because it strikes me, if the President says for day, after day, after day on T.V. that he doesn't have the authority and then now he does. I don't know, but I am just guessing that if that was somebody else that he didn't like that the President would say that person was lying, and has been lying for day, after day, after day.

I am just—I am just confused how the President can do that. And I know that, again, I know that you are going to carry out the orders, and I respect that, I really do, I respect that. But at some point, somebody at DHS, somebody at ICE is going to have to look in the mirror and ask themselves whether they want to keep doing this. Are you from Mass or just were lucky enough to go to B.C.?

Mr. NEVANO. No, I am from Massachusetts.

Mr. CAPUANO. And you—do you remember the name Elliot Richardson? Our former State Attorney General who became the U.S. Attorney General?

Mr. NEVANO. I am familiar with that name.

Mr. CAPUANO. Elliot Richardson quit. When the President of the United States ordered him to take action he found to be immoral, he quit his job. Now, I am not asking any line guy, 27-year-career guy to do that. That is a little much. But somebody somewhere at DHS and ICE, at some point, is going to have to ask themselves, when is it too much? When are the orders too much? I can't do them.

And, again, I am not suggesting it should be you or anybody in particular, and I really hate even putting that question to a career guy. I really would rather put that question to a political appointee, that would be people above your pay grade, and I get it, but again, and I apologize as I did earlier. I have to say some of these things to you, I don't really mean to direct them to you, you seem like a nice guy doing your job.

But until and unless we have access during a public forum to the people that can answer these questions, and can make those decisions, unfortunately you are stuck in. And I actually feel bad that your superiors put you in this position today to have to take this abuse. And I—and again, it is not directed to you, but I would be very clear, it is unequivocally directed to your superiors who do have the authority to say no, and should have said no to this policy. Thank you, Mr. Chairman.

Chairman PEARCE. The gentleman's time has expired. I would like to thank our witnesses for your testimony today. The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

This hearing is adjourned.

[Whereupon, at 3:43 p.m., the subcommittee was adjourned.]

A P P E N D I X

June 20, 2018

U.S. Immigration and Customs Enforcement

STATEMENT

OF

GREGORY C. NEVANO
DEPUTY ASSISTANT DIRECTOR
ILLICIT TRADE, TRAVEL, AND FINANCE DIVISION
HOMELAND SECURITY INVESTIGATIONS

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

"Illicit Use of Virtual Currency and the Law Enforcement Response"

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

Wednesday, June 20, 2018
2128 Rayburn House Office Building

Chairman Pearce, Ranking Member Perlmutter, and distinguished members:

Thank you for the opportunity to appear before you today to discuss the illicit use of virtual currency and the efforts of U.S. Immigration and Customs Enforcement (ICE) to target and investigate those who exploit virtual currency to carry out nefarious activity.

ICE's Homeland Security Investigations (HSI) has long stood at the forefront of combating transnational criminal activity that seeks to exploit our trade, travel, and financial systems for illicit purposes. HSI is the largest investigative agency within the U.S. Department of Homeland Security (DHS) with more than 6,000 special agents assigned to more than 200 domestic offices, and 67 international offices in 50 countries. HSI has authority to enforce more than 400 U.S. federal statutes, and some of our major investigative programs include financial crimes, counter proliferation, child exploitation, human smuggling and trafficking, narcotics smuggling, and intellectual property rights.

As a Deputy Assistant Director, I oversee the HSI Illicit Trade, Travel and Finance Division. The component of the Division overseeing our financial investigations is the Illicit Finance and Proceeds of Crime Unit (IFPCU). The IFPCU is one of many units within HSI which maintain equities addressing aspects of crime touching the virtual world. The primary focus of this Unit is to develop investigative techniques and typologies that help identify and eliminate vulnerabilities in the U.S. financial systems as well as provide HSI field offices the training and tools to pursue perpetrators of financial crimes. The IFPCU enhances cooperation and forges partnerships with domestic and foreign law enforcement, regulatory agencies, and non-governmental bodies to combat all types of financial crimes, to include the illicit use of virtual currencies to launder criminal proceeds. We also work alongside the U.S. Department of the Treasury and other government entities to provide anti-money laundering (AML) assessments, training, best practices, and lessons learned in the fight against global money laundering.

Positioned within the IFPCU is the Illicit Digital Economy Program (IDEP), forming the vanguard of HSI's investigative portfolio to counter the illicit use of virtual currency. Formed in 2013, the program was established to combat the money laundering and criminal exploitation of the rapidly emerging digital economy by Transnational Criminal Organizations (TCOs).

Rapid Growth of Virtual Currency

In 2009, bitcoin was introduced as the first decentralized convertible virtual currency. Bitcoin, like many convertible virtual currencies, is a "cryptocurrency." With its introduction, an entirely new world was created in relation to money laundering and financial investigations. Today, cryptocurrency has become more accepted for legitimate use in both commerce and investment. Bitcoin, for example, is accepted as a method of payment by hundreds of traditional brick and mortar stores as well as online merchants. There are currently more than 1,550 different cryptocurrencies in existence. Bitcoin is, by far, the largest and most widely accepted cryptocurrency.

Following its introduction, bitcoin quickly became the currency of choice on the Darknet as buyers and sellers enjoyed the pseudo-anonymity it provided. HSI continues to be a lead agency involved in the investigation and subsequent dismantling of several Darknet market places, including Silk Road and AlphaBay. The illicit use of cryptocurrency is not limited to use as a method of payment on Darknet market places. The pseudo-anonymity and ease of transfer cryptocurrency provides have led to expanded use by traditional criminal organizations with ample opportunity for expansion as it becomes more mainstream. The illicit use of cryptocurrency is found in many programmatic areas and case categories. Any crime committed for financial gain has the potential to involve cryptocurrency. Therefore, HSI does not treat the use of cryptocurrency for illicit purposes as a cybercrime, but rather as an online-enabled financial crime.

HSI's Lines of Effort

Financial Investigations:

Despite the pseudo-anonymity exploited by the users of bitcoin and other cryptocurrencies, as well as their ease of transfer, at some point criminals need to convert their cash into cryptocurrency or their cryptocurrency into cash. Whenever monetary exchanges are made, a chokepoint is created. This is the time when criminals are most vulnerable and can be identified by law enforcement means and methods. Utilizing traditional investigative methods such as surveillance, undercover operations, and confidential informants, coupled with financial and blockchain analysis, HSI is able to disrupt and dismantle the criminals and TCOs utilizing cryptocurrencies.

Most lawful users of cryptocurrencies are more than willing to conduct business with a cryptocurrency exchange that complies with Federal legal requirements. Many exchanges are registered with the U.S. Department of the Treasury's Financial Crimes Enforcement Network which issued guidance in 2013 clarifying that persons or companies involved in the exchange of cryptocurrency are money services businesses (MSBs) and making clear that exchanges must follow the same regulatory and reporting protocols as traditional MSBs. The protocols include developing and implementing an AML compliance program, filing suspicious activity reports, and registration protocols. These procedures are implemented to record personal identifying information from customers. Most lawful users are more than willing to provide personal identifying information and traditional financial institution account numbers in exchange for security, the lowest fees, and the ease of processing transactions.

Those who use cryptocurrency for illegal purposes, however, stay away from registered exchanges in an attempt to conceal their own identities. Instead, these criminals look to illicit or unregistered exchanges that do not require or ask for personal identifying information. These illicit exchanges often take the form of a direct Peer-to-Peer (P2P) exchanger. P2P exchangers post advertisements stating the price for which they are willing to either buy or sell cryptocurrency on websites like Craiglist and others. Although some P2P exchangers do register and follow compliance laws, most do not. Rather, these illicit P2P exchangers position themselves as the money launderers of the cryptocurrency world. One type of P2P exchanger illegally generates revenue by charging a premium for allowing their customers to remain

anonymous. They will sell cryptocurrency above market value and buy below market value to or from those customers who want to remain anonymous. Targeting these illicit P2P exchangers helps to open the door and pull back the veil of pseudo-anonymity provided by cryptocurrencies. Through interviews and suspect cooperation, along with forensic analysis of computers, mobile phones, and other seized electronics, as well as the use of advanced blockchain tracing tools, HSI can identify other criminals using cryptocurrency to fund and further their illicit activities.

Collaboration:

HSI Special Agents have always made it a practice to work cooperatively with federal, state, local, and international partners to investigate criminal networks operating around the globe. We use both established investigative techniques and models that have gradually evolved to keep pace with changing methodologies of TCOs. More so, HSI investigators are always on the lookout for innovative investigative approaches and the next developing threat over-the-horizon. Due to the rapidly increasing transformative nature of technology, it is more essential than ever that law enforcement agencies enhance their adaptability and fluidity when combating transnational crime. Nowhere is this more apparent than in the rapidly expanding world of cybercrime and online-enabled financial crime.

HSI participates in and has representation on dozens of collaborative cyber-related efforts, including the HSI Cyber Crimes Center, the Federal Bureau of Investigation's National Cyber Investigative Joint Task Force, the U.S. Secret Service Electronic Crimes Task Force, and the DHS Science and Technology Internet Anonymity Project Working Group.

HSI is combating the threat posed by the illicit manipulation of the cryptocurrencies through a multi-layered approach. By utilizing our broad authorities, HSI has dedicated units that are responsible for responding to this growing threat. Our IFPCU is responsible for investigating the movement and laundering of cryptocurrencies, our Cyber Crimes (C3) and Intellectual Property Rights Centers are responsible for monitoring bad actors located on the Darknet; our HSI agents assigned to EUROPOL coordinate multi-lateral foreign investigations of the Darknet, cryptocurrencies, and illicit travel connected to terrorism.

Training:

Like most law enforcement agencies, HSI has been engaged in a multiyear effort to increase its "cyber-enabled" workforce by training special agents, intelligence research specialists, and computer forensic analysts to conduct online investigations. The HSI IFPCU and the HSI Cyber Crimes Unit have partnered to conduct cryptocurrency and Darknet training for HSI agents and federal, state, local, tribal, and international partners. Special agents from HSI headquarters and field office subject matter experts conduct this specialized training. The training course "Cryptocurrencies and the Dark Web" is coordinated under the IDEP, has been well received, and to date in Fiscal Year (FY) 2018, HSI has conducted more than 50 outreach and training sessions, both nationally and internationally, reaching over 4,000 law enforcement, prosecutorial, judicial and other government personnel. Most recently, HSI has provided training in North Dakota where we had attendees from 18 different investigative agencies and

police departments; to Ohio with 400 attendees; and to Buffalo with 175 federal, state, and Canadian law enforcement partners.

This training enables U.S. law enforcement agencies to initiate prolonged and combined campaigns of coordinated investigations targeting the criminal organizations that are utilizing cryptocurrencies to launder illicit proceeds derived from various criminal schemes, to include fentanyl and opioid smuggling. HSI will continue this training and intends to follow up this course with intermediate and advanced-level training.

Outreach:

HSI abides by the belief and instills in its investigators that the "cornerstone" of virtually every investigation is financial. In 2003, HSI initiated the Cornerstone Outreach Initiative. Cornerstone is HSI's comprehensive initiative focused on financial investigations and with a primary outreach goal of detecting and closing vulnerabilities within the U.S. financial, trade, and transportation sectors. This mission is accomplished through proactive outreach and collaboration with businesses and industries that manage the very systems terrorists and other criminal organizations seek to exploit. Within the financial sector, HSI's efforts focus on conducting outreaches with traditional financial institutions as well as MSBs. With the rapid growth of cryptocurrency, and with it the expansion of private companies involved in cryptocurrency, HSI has expanded Cornerstone to include a directed effort to conduct outreaches and training with private industry involved in the cryptocurrency space. The private sector represents America's first line of defense against money laundering and the illicit use of cryptocurrency, which is why HSI partners with the business community, along with state and federal agencies, to combat financial crimes through a 21st century approach to law enforcement.

Investigative Successes and Statistics

Since the creation of cryptocurrency, HSI has steadily increased our knowledge, commitment, and capacity to combat money laundering regardless of the currency platform being used. HSI investigations into cryptocurrency have increased from one investigation initiated in FY 2011, to 203 investigations initiated in FY 2017. As of May 2018, HSI offices have initiated 144 cryptocurrency investigations, in addition to those already open and ongoing investigations. With the increase in our investigations, HSI has also seen a large increase in our seizures of cryptocurrency. For example, in FY 2014, HSI seized $151,459 in cryptocurrency. By the end of FY 2017, HSI seized $6,953,642 in cryptocurrency. Through the end of April 2018, HSI has already seized $25,442,611 in cryptocurrency.

I would like to take a moment to discuss some great HSI investigations involving the use of cryptocurrency and illicit Darknet sites. Like traditional robbery schemes aimed at pilfering a drug trafficker's profits, illicit Darknet sites and their virtual wallets can be compromised by various electronic methods aimed at stealing and diverting cryptocurrency. In 2013, in a multi-jurisdictional effort, HSI offices obtained indictments and arrest warrants for two online criminals who were electronically stealing cryptocurrency from an illicit Darknet site and then laundering the stolen currency through a series of virtual transfers. This HSI investigation

resulted in the seizure of a total of $4.5 million in virtual and hard currency that was stolen from the illicit site.

In another example, in July 2016, HSI Salt Lake City, Utah initiated a criminal investigation involving a TCO responsible for filling drug orders for regulated items such as Xanax through the Darknet. The investigative lead was forwarded to HSI by a cryptocurrency exchanger as a result of our Cornerstone initiative. The TCO dispensed approximately 1.8 million pills, half of which were laced with fentanyl. The TCO was responsible for thousands of drug laden postal shipments which were sent to almost every state in the nation. In November 2016, HSI agents received indictments and arrests warrants for seven members of the TCO and seized a total of $7,000,000 in virtual and hard currency as well as thousands of fentanyl laced pills and pill presses.

In March 2017, HSI Special Agents in Philadelphia, working in conjunction with their state and federal partners, intercepted a parcel sent from China to a U.S. address. Execution of a search warrant on the parcel revealed that it contained a synthetic opioid derivative. Further investigation discovered that the Philadelphia suspect had previously received two dozen similar shipments, and was acting as a trans-shipper under the direction of the Chinese organization. The developing investigation revealed that the Chinese source of supply was responsible for sending opioid laden parcels to approximately 19 other countries. The Chinese supplier operated as an illicit vendor on the Darknet and the payments were being remitted through cryptocurrency.

Investigations such as these are regularly highlighted in our trainings and outreach. When we identify trends, typologies are formulated to give our investigators potential models to apply. Equally, investigators in the field provide feedback to our trainers on the latest investigative exploits. While every investigation is unique, the crossroads joining virtual and fiat currency have been cited as one of the important investigative junctures that law enforcement can exploit to disrupt and dismantle these criminal and smuggling organizations.

Challenges

Many new cryptocurrencies have been and will continue to be developed. Some newer cryptocurrencies have features that make the tracing of them quite complicated. These new anonymity-enhanced cryptocurrencies are clearly ripe for illicit use in an effort to subvert legitimate law enforcement inquires. Although it is more difficult to trace the movement of illicit proceeds using these newer anonymity-enhanced cryptocurrencies, it is not impossible. Regardless of the cryptocurrency used, by targeting the chokepoints and nodes where convertible cryptocurrency activities intersect with the regulated fiat currency financial system, HSI is confident that we will still be able to conduct successful investigations and identify those criminals and TCOs utilizing cryptocurrency for illicit purposes.

Technology will inevitably continue to evolve, and law enforcement agencies everywhere must continue to adapt and evolve as well. HSI will continue to partner with all law enforcement agencies, along with cutting-edge private technology partners, to stay ahead of the curve and

keep technologically savvy criminals on their heels. These vital partnerships are the foundation that allows law enforcement to continue its effort in combating TCOs on all fronts, including the emerging threat of online-enabled financial crimes.

Conclusion

Thank you again for the opportunity to appear before you today and for your continued support of U.S. Immigration and Customs Enforcement, Homeland Security Investigations, and our law enforcement mission. We will continue to use our unique and powerful combination of law enforcement authorities and access to information to close vulnerabilities that can be exploited to harm our homeland in the real and virtual worlds. ICE HSI is committed to protecting America from the cross-border criminal organizations seeking to exploit and undermine our financial systems, preventing terrorism and combating the illegal movement of people and goods.

I appreciate your interest in the burgeoning field of cryptocurrency and its impact on illicit endeavors, and look forward to any questions.

Robert Novy

Deputy Assistant Director
Office of Investigations
United States Secret Service

Prepared Testimony

Before the
United States House of Representatives
Committee on Financial Services
Subcommittee on Terrorism and Illicit Finance
June 20, 2018

Chairman Pearce, Ranking Member Perlmutter, and members of this Subcommittee: Thank you for inviting me to testify before you about the U.S. Secret Service's actions in response to the increasing illicit activities involving digital currencies.[1] The Secret Service's primary concern regarding this topic is digital currencies' use in criminal schemes that undermine the integrity of financial and payment systems, their use in cases of fraud, and their general use as a means of money laundering. The Secret Service possesses a unique record of success in countering criminal uses of digital currencies, and we are committed to continuing to keep pace with technology innovation, as well as evolving strategies and tactics, of cyber criminals. My testimony describes our observations on trends and patterns related to digital currency, as well as some of the challenges that may warrant Congressional attention.

As one of the nation's original investigative agencies charged with safeguarding the nation's financial and payment systems, the Secret Service has conducted criminal investigations to protect the American public, companies, financial institutions, and critical infrastructure from criminal exploitation since 1865. As early as 1982, the Secretary of the Treasury directed the U.S. Secret Service to investigate crimes related to electronic funds transfers, in order to keep pace with the growing role of computers in the U.S. financial system. Two years later, in 1984, Congress passed legislation to expand the Secret Service's responsibilities to include investigating a range of computer hacking and access device fraud violations. Today, we have extensive authorities to safeguard financial and payment systems from criminal exploitation, even as those illicit activities are increasingly transnational in nature and enabled by cyberspace and digital currencies.[2]

In executing our law enforcement mission, the Secret Service closely partners with Federal, state, local, and international law enforcement agencies, as well as with a range of other international and domestic partners. We do this in part through our network of Electronic Crimes Task Forces (ECTFs)[3] and Financial Crimes Task Forces. Specifically, as it relates to criminal investigations involving digital currency, we partner particularly closely with U.S. Immigration and Customs Enforcement's Homeland Security Investigations (ICE/HSI), the Financial Crimes Enforcement Network (FinCEN), the Federal Bureau of Investigations (FBI), and other Federal agencies with related responsibilities.

---

[1] The term "digital currency" is used to refer to a representation of value that is stored on and transferred through computer systems that is used similar to money (used as a medium of exchange, unit of account, store of value, or standard of deferred payment) and is used as a substitute for or converted to legal tender of the United States or another country. The term "digital currency" is closely related to "virtual currency" (as defined by the FinCEN Guidance issued 18 March 2013), but may also include digital currencies that are recognized as legal tender.

[2] Criminal activity related to digital currencies investigated by the U.S. Secret Service often involve violations relating to 18 U.S.C. §§ 1028, 1028A, 1029, 1030, 1343, 1956, 1957, 1960, and 3056(b).

[3] Section 105 of the USA PATRIOT Act of 2001 directed the Secret Service to establish a "a national network of electronic crimes task forces, … for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." The first Secret Service ECTF was established in New York in 1995; today the Secret Service operates 40 ECTFs, as part of an expanding international network that partners Federal, state, and local law enforcement with the private sector and academia to effectively investigate cyber crimes.

Since the commercialization of the Internet in the early 1990s, there have been various efforts to develop payment systems that can function effectively within the digital economy. The market has predominately adopted payment cards as this solution, but there have also been numerous attempts to establish digital currencies that operate with greater independence from the established financial system. While some digital currencies have operated lawfully, others have been used extensively for illicit activity.

The Secret Service has been at the forefront of investigating the illicit use digital currencies. Working with our interagency partners, we have investigated and shutdown two major centralized digital currencies that supported extensive criminal activity: e-Gold Ltd. (in 2007)[4] and Liberty Reserve (in 2013).[5] Since then, the Secret Service has worked with our partners to investigate and shutdown a number of illicit digital currency exchangers,[6] including Western Express, which was prosecuted by the Manhattan District Attorney's Office, and, in 2017, the cryptocurrency exchange BTC-e,[7] working in partnership with the Internal Revenue Service's Criminal Investigations (IRS-CI) and other law enforcement agencies. These, and numerous other criminal investigations, have provided the Secret Service with insight on the risks and challenges posed by digital currencies, and the effectiveness of various potential law enforcement responses.

Criminal Use of Digital Currencies

In recent years, criminals have increasingly used digital currencies to facilitate illicit activities on the Internet. Digital currencies provide an efficient means of transferring large values globally, for both legitimate and criminal purposes. Some providers, exchangers and users of digital currencies attempt to avoid the international legal and regulatory systems established to counter illicit finance. Based on Secret Service investigations into criminal use of digital currencies, criminals prefer digital currencies they assess to have the following characteristics:

1) Widespread adoption as a medium of exchange for intended criminal activities;
2) The greatest degree of anonymity.
3) Protection against theft, fraud, and lawful seizure.
4) Can be readily exchanged to and from their preferred currency.[8]

---

[4] *See* https://www.justice.gov/usao-md/pr/over-566-million-forfeited-e-gold-accounts-involved-criminal-offenses.
[5] *See* https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.
[6] Exchangers are businesses that allow for the trade of digital currencies for other assets, such as conventional fiat money, such as US dollars, or other digital currencies.
[7] *See* https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.
[8] The term "currency" is defined pursuant to 31 CFR 1010.100(m) as "The coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance. Currency includes U.S. silver certificates, U.S. notes

5) The ability to quickly and confidently transfer value transnationally.

There is a large number of digital currencies available today, but only a few have been substantially adopted for engaging in certain illicit activities. Some digital currencies are primarily used to purchase illicit goods and services (e.g., drugs, credit card information, personally identifiable information (PII), and other contraband or criminal services). Other digital currencies are primarily used for money laundering—particularly transnational transfers. The greatest risks are posed by digital currencies that have widespread use for both of these purposes. e-Gold and Liberty Reserve were prime examples of these risks. Both platforms effectively conducted no customer verification, and were extensively used for a range of illicit activities, from child exploitation to identity theft, before the Secret Service shut them down.

Use of a Blockchain as Digital Currency

In 2008, Bitcoin was proposed as a digital currency that could provide a decentralized payment system through use of cryptography to form a trusted chain of digital signatures, known as a blockchain.[9] Following the example of Bitcoin, beginning in 2011, various individuals and groups launched their own blockchain implementations that provide various other forms of cryptocurrencies.[10] As of 12 June 2018, there are over 600 blockchains in operation on the Internet and, based on current exchange prices, the total market capitalization of cryptocurrencies is approximately $290 billion. Currently, the four largest cryptocurrencies, by market capitalization, are: Bitcoin ($116 billion), Ethereum ($52 billion), Ripple ($22 billion), and Bitcoin Cash ($16 billion).[11] The Secret Service has adapted to this trend; for example, from FY 2015 to present, the Secret Service has seized over $28 million in cryptocurrencies in the course of our criminal investigations,[12] primarily in the form of Bitcoin.

In addition to the use of blockchains to provide a digital currency, various organizations are considering using blockchains for other purposes. These include a decentralized public ledger for tracking ownership of property, digital identity management, and supply chain management. For example, Ethereum, which provides a decentralized Turing-complete virtual machine (the Ethereum Virtual Machine, or EVM),[13]serves as platform for numerous decentralized applications and smart contracts. Ethereum has become one of the most popular platforms for

---

and Federal Reserve notes. Currency also includes official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country."

[9] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (31 October 2008). Available at: https://bitcoin.org/en/bitcoin-paper.

[10] The term "cryptocurrency" is used to refer to a decentralized system that uses cryptographic techniques to regulate the generation and transfer of a digital currency.

[11] *See* Coin Market Cap, "Top 100 Coins by Market Capitalization." Last accessed on 12 June 2018. Available at: https://coinmarketcap.com/coins/.

[12] Value at the time the seizure was executed.

[13] As a Turing-complete system, the EVM is able to compute every function general purpose computers are capable of—an important property in computer science.

conducting Initial Coin Offerings (ICOs). In 2017, approximately $3.88 billion was raised through Initial Coin Offerings.[14] The Secret Service partners with the Security and Exchange Commission (SEC) in addressing criminal risks related to ICOs, as the SEC has taken an active role in addressing risks to investors and businesses related to use of ICOs to raise capital and participate in investment opportunities.[15]

The growing popularity of blockchains has also resulted in the growth of criminal activities closely related to its proprieties. These include: crypto-jacking, thefts of private keys, ransomware, and attacks on blockchain networks themselves. Crypto-jacking is the use of malware or compromised websites to use, without authorization, computing power of others for cryptocurrency mining.[16] Control of assets on a blockchain is maintained through exclusive control and access to the associated private cryptographic key; however, there have been numerous instances of cryptocurrency heists, involving major exchanges, wallets and individual users resulting from the theft and illicit use of private cryptographic keys. While ransomware, which impairs the operation of a computer as part of an extortion demand, has been around since the late 1980s, its growth over the last four years has substantially been driven by use of cryptocurrencies as the means of paying extortion demands. Finally, we have observed a few instances of attacks on blockchain systems themselves, either to impair their operation, as part of a broader scheme, or as part of a "51% attack"[17] to defraud other users of the cryptocurrency. All such activities typically involve violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) and potentially other criminal statutes.

Exchangers of cryptocurrency have been a particularly effective control point for law enforcement to focus its effort. For example, BTC-e was Internet-based, foreign-operated money transmitter that exchanged fiat currency as well as convertible cryptocurrency such as Bitcoin. Before it was shut down as part of a multi-national law enforcement operation, it was one of the largest digital currency exchanges by volume, receiving $4 billion worth of digital currency over the course of its operation from 2011 to 2017. BTC-e processed transactions involving the criminal proceeds of numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials and narcotics distribution rings. BTC-e also allegedly facilitated the exchange of roughly 95 percent of ransomware payments, according to a non-government report.

Challenges related to Digital Currencies and Potential Congressional Actions

[14] Coinschedule, "Cryptocurrency ICO Stats 2017." Last accessed on 12 June 2018. Available at: https://www.coinschedule.com/stats.html?year=2017.
[15] *See* https://www.sec.gov/ICO.
[16] Mining is the computational process that verifies and maintains a blockchain, and is typically incentivized by a blockchain protocol rewarding cryptocurrency to miners.
[17] A "51% attack" is scheme whereby over 50% of the computational power participating in a blockchain is used in a concerted manner that undermines the integrity of that blockchain.

The growing illicit use of digital currencies risks undermining the effectiveness of existing U.S. laws and regulations, especially those intended to limit the ability of criminals to profit from their illicit activities. The key U.S. laws relevant to Secret Service investigations involving the illicit uses of digital currencies include the Bank Secrecy Act of 1970, the Annunzio-Wylie Anti-Money Laundering Act, the Money Laundering Suppression Act of 1994, and Title III of the USA PATRIOT Act of 2001, in addition to other associated laws and Federal regulations. Congressional attention to the positive effects of these laws is especially needed today, as we are in a period of significant technology innovation within the financial sector.

Given the global nature of the Internet and modern communications, digital currencies are particularly well-suited for supporting crimes that are transnational in nature. Accordingly, effectively countering criminal activity involving digital currencies requires close international partnerships. Foreign partners play key roles in assisting U.S. law enforcement with conducting investigations, making arrests, and seizing criminal assets. Fostering these partnerships and conducting these transnational investigations requires continual investment in international law enforcement collaboration, and a persistent effort to harmonize anti-money laundering laws and related criminal statutes. It is critical that the United States continues to work internationally to improve controls related to digital currency through organizations like the Financial Action Task Force.[18] We should also consider additional legislative or regulatory actions to address potential challenges related to anonymity-enhanced cryptocurrencies, services intended to obscure transactions on blockchains (i.e. cryptocurrency tumblers or mixers) and cryptocurrency mining pools.

Some businesses, including providers of information and communications systems, are taking actions that impede timely access to digital evidence. As such, continued Congressional attention is warranted to ensure law enforcement agencies maintain lawful access to critical sources of evidence, regardless of where, or in what form, that information is stored. The recently enacted CLOUD Act was an important step in this regard, but further legislative or regulatory action may be needed, as case law and business practices continue to develop. Such legislative or regulatory actions could take the form of new reporting requirements or data collection, retention, and accessibility requirements for certain businesses or business activities.

Further, investigating crimes involving digital currencies, and the transnational organized cyber criminals that extensively use them, requires highly skilled criminal investigators. Hiring, developing, and retaining our investigative workforce, as well as partnering with and training our law enforcement and private sector partners to develop robust investigative capabilities, are all critical priorities for ensuring we are well prepared to address emerging risks resulting from technology innovation, both today and into the future.

[18] *See* http://www.fatf-gafi.org/.

Conclusion

Despite these challenges, we are committed to continuing to effectively execute our mission. Digital currencies have the potential to support more efficient and transparent global commerce, and to enhance U.S. economic competitiveness. However, because digital currencies continue to be used to facilitate illicit activity, law enforcement must adapt our investigative tools and techniques to dismantle criminal groups that use these instruments for fraudulent activity or money laundering.

Those that seek to further their illicit activities through use of digital currencies should have no illusions that they are beyond the reach of the law. As the investigative work of the Secret Service and our law enforcement partners continues to demonstrate, we are relentless in enforcing the law and will not be stopped by the perceived anonymity of the Internet or digital currencies.

Testimony for the Record
Thomas P. Ott
Associate Director, Enforcement Division
Financial Crimes Enforcement Network
U.S. Department of the Treasury
House Committee on Financial Services
Subcommittee on Terrorism and Illicit Finance
June 20, 2018

Introduction

Chairman Pearce, Ranking Member Perlmutter, and members of the Subcommittee, thank you for inviting me to appear before the Subcommittee on Terrorism and Illicit Finance on behalf of the Financial Crimes Enforcement Network (FinCEN). FinCEN's mission is to safeguard the financial system from illicit use and to promote national security through the collection, analysis, and dissemination of financial intelligence.

I appreciate the opportunity to discuss Treasury's work on virtual currency and the national security implications and illicit finance risks presented by virtual currency.

FinCEN, together with other components of U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence, or TFI, works to combat the illicit finance threats presented by both traditional and emerging payment systems. In doing so, our aim remains to deter, detect, and disrupt illicit finance threats from the financial system while promoting responsible technological innovation in the financial sector.

FinCEN's Regulatory Treatment of Virtual Currency

The United States has led the world in regulating and supervising virtual currency payments, including decentralized virtual currency payment activities, for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes. Treasury has worked on issues pertaining to virtual currency since the early 2000s. At the federal level, FinCEN, which has the primary responsibility for administering the Bank Secrecy Act (BSA) and implementing its regulations, regulates individuals or entities engaged in the business of accepting and transmitting virtual currency from one person to another person or location as money transmitters.

Most importantly, in 2011, FinCEN issued a final rule, which among other things, defined "money transmission services" to include accepting and transmitting "currency, funds, or other value that substitutes for currency" by any means.[1] The term "other value that substitutes for currency" is intended to encompass circumstances in which the transmission does not involve

[1] Bank Secrecy Act Regulations - Definitions and Other Regulations Relating to Money Services Businesses, 76 FR 43585 (July 21, 2011). *See* also 31 CFR § 1010.100(ff)(5)(i)(A).

currency as defined by regulation, [2] or funds, but instead involves something that the parties to a transaction recognize has value that is equivalent to or can substitute for real currency. The definition of money transmission is technology neutral: whatever the platform, protocol, or mechanism, the acceptance and transmission of value from one person to another person or location is regulated under the BSA.

The 2011 rule establishes the foundation for our regulation of certain virtual currency activity and sets out the obligations of financial institutions that are money transmitters of virtual currency under the BSA.

FinCEN established that money services businesses (MSBs) that conduct money transmission denominated in other forms of value, such as virtual currency, are obligated to meet the same AML/CFT standards as other money services businesses under the BSA. This includes registering with FinCEN, establishing an AML program reasonably designed to prevent money laundering and terrorist financing, and meeting certain recordkeeping and reporting obligations—including filing Suspicious Activity Reports (SARs). The requirements apply equally to domestic and foreign-located virtual currency money transmitters, even if the foreign-located entity does not have a physical presence in the United States, as long as it does business in whole or substantial part in the United States.

To provide additional clarity and respond to questions from the private sector, in March 2013, FinCEN issued interpretive guidance on the application of FinCEN's regulations to certain transactions involving the acceptance of currency or funds and the transmission of virtual currency ("2013 Guidance"). [3] The 2013 Guidance identified the participants to some virtual currency arrangements, including an "exchanger," "administrator," and "user," and further clarifies that exchangers and administrators generally qualify as money transmitters under the BSA, while users do not. FinCEN has subsequently issued several administrative rulings providing additional clarity on virtual currency matters including, but not limited to, discussing virtual currency issues such as mining[4] and operating a virtual currency-trading platform.[5] FinCEN expects financial institutions, including those operating in virtual currency, to comply with FinCEN's regulations. This may require them to proactively evaluate their business models using the guidance and rulings that FinCEN publishes. Financial institutions that consult the regulations and guidance but are still uncertain as to whether their particular business model falls

---

[2] 31 CFR § 1010.100(m) (Defines currency as "[t]he coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance. Currency includes U.S. silver certificates, U.S. notes and Federal Reserve notes. Currency also includes official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.").

[3] FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013.

[4] FIN-2014-R001, "Application of FinCEN's Regulations to Virtual Currency Mining Operations," January 30, 2014.

[5] FIN-2014-R011, "Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform," October 27, 2014.

within FinCEN's regulations may seek formal and informal regulatory interpretations from FinCEN.

Illicit Finance Risks

Fundamentally, we must maintain the integrity and accessibility of the global financial system and protect it from abuse. Virtual currency payments pose money laundering, sanctions evasion, and other illicit financing risks that necessitate careful assessment and mitigation. In particular, we are concerned about the growing use of decentralized convertible virtual currency to facilitate illicit activity, including cybercrime, fraud, extortion, drug trafficking, money laundering, and other crimes.

We have seen virtual currency exploited to support billions of dollars in what we would consider suspicious activity. For example, FinCEN analysis indicates that virtual currency transactions include over $1 billion in ransomware extortion funds and over $1.5 billion has been stolen through hacks of virtual currency exchangers and administrators over the past two years. FinCEN analysis also estimates that at least $4 billion in virtual currency has moved through darknet marketplaces since 2011.

While traditional financial methods remains the primary vehicle for most illicit activity, FinCEN believes virtual currency presents specific illicit finance risks and that without vigilance and action, the scale of this activity could grow.

In fact, we have seen an increase in SAR filings by financial institutions identifying illicit virtual currency activity. Since 2003, BSA information identifying suspicious activity involving virtual currency has grown rapidly, increasing 90 percent from 2016 to 2017. These reports have identified many thousands of virtual currency addresses tied to a wide range of suspected criminal activity and have proven immensely useful to investigations. This reporting has directly assisted important criminal and civil actions taken by law enforcement and regulators in the United States.

International Regulation

Foremost among our challenges in combatting this activity is the lack of consistent AML/CFT regulations and supervision of virtual currency activity in most jurisdictions around the world. The global nature, distributed structure, and speed of most leading virtual currency systems means that vulnerabilities in foreign jurisdictions can enable illicit activity here in the United States. Success cannot come without concerted action in the international community. We have seen great strides to address this regulatory gap in places like Australia, Japan, and South Korea, but most jurisdictions still do not have a regulatory framework in place or in-progress to address virtual currencies. Until jurisdictions ensure that these businesses adhere to the same international AML/CFT standards as other financial institutions, there will be vulnerabilities that expose the U.S. to illicit finance risks. Bad actors will continue to seek jurisdictions that permit illicit behavior and find ways to offer their services around the world.

FinCEN and other Treasury components are working to engage key jurisdictions directly and help them address these vulnerabilities in their AML/CFT regime. Our experts have provided training directly to foreign regulators and law enforcement to improve their oversight and understanding of these technologies, and will continue to conduct outreach and engagement in this area.

Further, through international standard setting bodies like the Financial Action Task Force (FATF), the United States has prioritized establishing and applying international standards for AML/CFT that cover virtual currency payments. Under the FATF Recommendations, countries should identify and assess the money laundering and terrorist financing risks in their jurisdictions related to virtual currency activities and adopt risk-based measures to mitigate those risks. Prompt and effective implementation and enforcement of the FATF AML/CFT requirements for virtual currency exchangers, hosted wallets, and similar businesses by all jurisdictions are vital for combatting the abuse of virtual currency and promoting safe, responsible innovation in the financial sector. We are pressing for jurisdictions to effectively regulate and supervise virtual currency exchangers, hosted wallets, and other virtual currency businesses that act as gateways to the regulated fiat financial system, in compliance with the international standards set by the FATF.

Anonymity-Enhanced Cryptocurrencies

There have also been developments in technology that have enabled the concealment of transaction and identity information involving virtual currency. Anonymity-enhanced cryptocurrencies (AECs)—sometimes referred to as "privacy coins"—are increasingly prevalent across exchange platforms and average around $300 million in daily transaction volume at domestic and foreign-located exchanges. We have seen AECs gain greater adoption by criminals looking for alternatives to bitcoin on darknet marketplaces. For example, AECs were adopted by the darknet marketplace AlphaBay prior to its shut down by U.S. law enforcement last year and U.S. law enforcement seized AECs from Alexander Cazes, the site's administrator.

Combating Illicit Virtual Currency Use

As part of developing and rigorously enforcing one of the most effective AML/CFT regimes in the world, FinCEN has increasingly prioritized identifying, tracing, and disrupting the flow of illicit virtual currency activity. But, as strong as our AML/CFT framework is, malicious actors will continue to attempt to exploit any vulnerability to move their illicit proceeds undetected through legitimate financial channels, in order to hide, foster, or expand the reach of their criminal or terrorist activity.

Supervision and Examinations

One of the ways FinCEN protects the financial system is by examining financial institutions for compliance with their regulatory obligations in preventing money laundering and terrorist financing. FinCEN has provided training to our delegated examiners, the Internal Revenue Service's (IRS) Small Business/Self-Employed Division. And, since late 2014, the IRS, together with FinCEN, has conducted examinations of virtual currency exchangers and administrators

across the United States. In that time, more than one-third of all registered virtual currency money transmitters in the United States have been examined, including numerous trading platforms, foreign-located exchangers, virtual currency kiosk companies, individual peer-to-peer exchangers, and five of the 20 largest exchanges by volume. Our goal is to ensure that virtual currency exchangers and administrators are subject to the same routine compliance examinations for AML/CFT as any other financial institution.

This year FinCEN has also provided virtual currency examination training to a number of state examiners, so that we can increase the reporting we receive of AML/CFT deficiencies and provide better oversight of this industry.

As with our BSA supervision of other parts of the financial services industry, these exams help FinCEN determine whether virtual currency exchangers and administrators are meeting their compliance obligations under the applicable rules. Where we identify problems, we will use our supervisory and enforcement authorities to appropriately penalize non-compliance and drive compliance improvements. Compliance only works with an effective enforcement regime.

Enforcement Actions

FinCEN has also taken significant public actions. For example, in 2013, FinCEN identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act. Liberty Reserve, a Costa Rica based administrator of the virtual currency LRDollars and LREuros, processed billions of dollars of criminal proceeds including from hackers and extortion schemes and sought to provide anonymous money laundering services to criminals around the globe. FinCEN imposed special measure five under Section 311, prohibiting U.S. financial institutions from opening or maintaining correspondent accounts with Liberty Reserve, thereby shutting it out of the U.S. financial system.

In 2015, FinCEN took its first civil enforcement action against a virtual currency business, imposing a $700,000 civil money penalty against Ripple Labs in coordination with a concurrent action by the U.S. Attorney's Office for the Northern District of California. FinCEN's action identified that Ripple Labs had operated as an unregistered MSB, had AML program failures, and failed to file SARs. Importantly, in addition to the penalty, Ripple Labs agreed to implement a remedial framework designed to bring the company into compliance with the BSA – a framework they remain under to this day. In taking this action, FinCEN wanted to provide a clear path of what compliance looks like. Our ultimate goal is not to shut down every virtual currency actor, but rather to ensure that all virtual currency entities meet AML/CFT standards.

However, we are not afraid to single out bad actors and take action. Most recently, in July 2017, FinCEN assessed a penalty of over $110 million against BTC-e; an internet-based, foreign-located money transmitter that exchanged fiat currency as well as the virtual currencies Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash. This action was taken with a parallel criminal action by our law enforcement partners including the Federal Bureau of Investigation, United States Secret Service, and Homeland Security Investigations, as well as those at Main Justice and the U.S. Attorney's Office for the Northern District of California. At the time, it was one of the largest virtual currency exchanges by volume in the world. BTC-e

facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. As part of this action, FinCEN also assessed a $12 million penalty against one of BTC-e's operators – the highest penalty we have ever assessed against an individual.

Collaboration

Collaboration is critical to combat the growing threats presented by virtual currency. To further collaboration across the financial sector, Secretary Mnuchin has convened a working group through the Financial Stability Oversight Council to bring together federal financial regulators whose jurisdictions are relevant to the oversight of virtual currencies and their underlying technologies. The working group seeks to enable the agencies to collaborate regarding these issues, including to promote consistent regulatory approaches and to identify and address potential risks.

Along these same lines, Under Secretary Mandelker has created Strategic Impact Units to combine the expertise of all TFI components to address various illicit finance challenges, including those posed by virtual currency. We have also increased our collaboration with our law enforcement partners, including those represented with me today, as well as our regulatory partners.

Just last month, I met with my enforcement counterparts at the Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC). My staff, and others at FinCEN, carefully and closely coordinate with these agencies on an ongoing basis in order to best allocate our resources to assess and address the greatest threats. This partnership has been fruitful, and the benefits are apparent through the excellent respective work by the SEC, CFTC, and FinCEN in targeting illicit actors and combating fraud related to the misuse of virtual currencies.

One area where we continue to work together is on the illicit finance risks surrounding Initial Coin Offerings (ICOs). As my SEC[6] and CFTC[7] colleagues have pointed out at prior hearings, this issue has gained a lot of attention from the public, and ICOs have experienced rapid growth since 2017. While ICO arrangements vary and, depending on their structure, may be subject to different authorities, one fact remains absolute: FinCEN, and our partners at the SEC and CFTC, expect that businesses involved in ICOs meet all of their AML/CFT obligations. We will remain committed to take appropriate action when these obligations are not prioritized and the U.S. financial system is put at risk.

I also want to highlight the important collaborations we have with our partners in law enforcement. We are extremely fortunate to have a team of experts within FinCEN who work very hard to keep pace with the quickly evolving technology in this area. We share that

[6] Jay Clayton, Chairman, U.S. Securities and Exchange Commission, Testimony before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Feb. 6, 2018.

[7] J. Christopher Giancarlo, Chairman, Commodity Futures Trading Commission, Testimony before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Feb. 6, 2018.

knowledge and analysis with law enforcement, regulators, and prosecutors domestically and globally, as we are all on the front lines of investigating illegal use of emerging payment systems.

To that end, FinCEN has provided support to over 100 cases since 2016. FinCEN's experts help law enforcement, regulators, and prosecutors trace different types of virtual currency activity, identify suspicious sources of funds, target unregistered MSBs that do business in whole or substantial part in the United States, and disrupt transnational criminal networks operating in virtual currency. To assist in tracing virtual currencies, FinCEN analysts produce detailed reports on typologies and methodologies addressing the movement of funds and the techniques used to launder illicit proceeds using virtual currency. FinCEN leverages the BSA data we receive from financial institutions to support law enforcement and develop our understanding of the threats. We also use our knowledge and resources to provide training to our law enforcement partners and help identify best practices for tracing funds and building cases.

Conclusion

As we continue to see technology evolve and integrate into the U.S. and global financial system, we must ensure that it does so in a way that allows for the transparency needed to protect the financial system. FinCEN looks forward to working with this Committee, the public sector, law enforcement, the intelligence community, and our regulatory partners to identify strategies to help ensure the United States remains both a global hub for innovation and a safe and secure financial system. Thank you for having me here today. With your support, FinCEN will continue combatting money laundering and illicit finance threats to secure our financial system, keep our nation safe and prosperous, and protect our communities and families from harm. I am happy to answer any questions you may have.

Department of Justice

STATEMENT OF

STEVEN M. D'ANTUONO
ACTING DEPUTY ASSISTANT DIRECTOR
CRIMINAL INVESTIGATIVE DIVISION
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON TERRORISM AND ILLICT FINANCE
COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

FOR HEARING ENTITLED

"ILLICIT USE OF VIRTUAL CURRENCY AND THE LAW ENFORCEMENT RESPONSE"

PRESENTED

JUNE 20, 2018

Statement of
Steven M. D'Antuono
Acting Deputy Assistant Director
Criminal Investigative Division
Federal Bureau of Investigation
Department of Justice

Before the
Subcommittee on Terrorism and Illicit Finance
Committee on Financial Services
U.S. House of Representatives

For a Hearing Entitled
"Illicit Use of Virtual Currency and the Law Enforcement Response"

Presented
June 20, 2018

Chairman Pearce, Vice Chairman Pittenger, and esteemed members of the Subcommittee, I am pleased to submit this statement for the record for today's hearing on the illicit use of virtual currency. Unfortunately, I am unable to attend today's hearing. However, I am thankful to have the opportunity to share this statement which covers three primary topics: the FBI's evaluation of virtual currency; investigative obstacles the FBI is facing regarding the illicit use of virtual currencies; and how the FBI is addressing threats posed by the illicit use of virtual currency.

The FBI has long served as a preeminent law enforcement agency, particularly in regard to financial crimes. Formulated in 1908 and recognized for many infamous gangster, kidnapping, and bank robbery investigations in our early days, a majority of our initial special agents were accountants and attorneys primarily charged with the investigation of mostly white-collar matters such as antitrust and bank fraud. The FBI has continued to build on that strong foundation and continues today our prioritization of financial crimes, working diligently on behalf of the American people to address crime problems that have grown in their complexity and scope. These crimes often cross international borders and use the latest advancements in technology and innovation.

Criminals today are increasingly using new technologies to support their illicit activities. They often hide behind the veil of anonymity that virtual currencies and places like the Darknet can afford them. We see that drugs are no longer sold just on the streets; fentanyl and opioids are now being shipped to doorsteps across this nation through online marketplaces using virtual currencies. New virtual currencies are being fraudulently offered to take advantage of the public's growing interest in these new investment opportunities, and all types of criminals can now quickly launder and move illicit funds around the world with enhanced anonymity. But just as criminal methods have evolved, so too has the FBI. We are more committed than ever to increasing our knowledge of these emerging threats so that we can effectively combat them.

The FBI recognizes the necessity for flexibility and collaboration internally, as well as with our law enforcement and regulatory partners. We lead 528 domestic task forces and numerous ad hoc working groups dedicated to combating criminal threats. These partnerships serve as a force-multiplier to address the variety of threats we face, from advancements in money laundering, to virtual currency investment frauds, to the growth of online illicit opioid trafficking.

To that end, the FBI has partnered closely with our domestic and foreign partners through task forces, working groups, and parallel working relationships to address these threats. In concert with those partnership efforts, the FBI is formulating new ways to combat growing technologically advanced criminal activity given our wide ranging expertise. For example, the FBI recently established the High Tech Organized Crime Unit, which focuses on increasing our ability to combat criminals who exploit technology and our financial systems to conduct traditional criminal activity such as money laundering, computer-enabled fraud, and drug trafficking. Through this unit, the FBI is leading the Department of Justice's Joint Criminal Opioid Darknet Enforcement ("J-CODE") team, which is targeting the use of virtual currencies in online opioid trafficking.

To date, the FBI has dedicated over 4,500 agent resources across 56 field offices to address all manners of financial crimes, as well as over 1,600 forensic accountants, intelligence analysts, and professional staff dedicated to addressing these crimes. The FBI has prioritized our efforts to train our personnel and ensure our agency is capable and equipped to address criminals who seek to take advantage of new technologies such as the virtual currencies we are discussing today.

The FBI's Position on Virtual Currency

The FBI recognizes that there are many legitimate and practical uses of virtual currency. Moreover, as a leading federal law enforcement agency for the investigation of financial crimes, we find that a subject's use of virtual currency can sometimes provide evidence that does not exist in traditional financial transactions. That is because every transaction involving a virtual currency is tracked. Bitcoin, for example, maintains a public ledger detailing every transaction. Furthermore, once a subject's virtual currency address or addresses have been affixed to him or her, law enforcement may then be able to identify a litany of additional transactions he or she previously made. In contrast to cash and other types of payment systems, where no transaction records may exist, virtual currency transactions are sometimes favorable for law enforcement.

There are many entities in the virtual currency industry working with the FBI to implement strong Know Your Customer ("KYC") standards for users of their systems. Many of these entities are instrumental exchangers between traditional fiat currencies and virtual currencies, or exchangers among two different virtual currencies, e.g. Bitcoin to Ethereum. Businesses that accept and transmit virtual currency, and must be registered as money service businesses ("MSB") and are subject to regulation by the Financial Crimes Enforcement Network

("FinCEN"). These registered MBSs must follow the Bank Secrecy Act ("BSA") and collect and maintain KYC data and respond to legal process, similar to a traditional financial institution. The information they provide assists us with identifying individuals and entities involved in suspect virtual currency transactions. The FBI has had success obtaining records from both domestic and foreign based entities. However, it should be noted that there are MSBs operating in the United States and abroad that do not collect adequate customer records and do not respond to legal process requesting customer records. The FBI addresses this vulnerability through investigations into entities operating unregistered MSBs.

Overall, the importance of customer records and data held by virtual currency money transmitters cannot be overstated. That information is vital to our investigations involving virtual currencies, and it is the key to law enforcement's ability to attribute virtual currency transactions to particular individuals.

Another common topic of concern related to the use of virtual currency is its association with and exacerbation of activity on Darknet marketplaces, including its use in the sale of illegal substances like heroin and fentanyl. A 2017 Global Drug Survey found that approximately ten percent of all drug users worldwide are now acquiring their personal-use drugs online. In addition to drug commerce, these marketplaces are also saturated with money laundering services, fraud services, and the retailing of other dangerous substances like weapons and poison. While these marketplaces are certainly troubling and have justifiably made headlines across the globe, they offer us unique opportunities for identifying and neutralizing illicit vendors, who would otherwise likely remain concealed.

One of the primary techniques of all investigations involving the sale of illicit products is tracing illicit money movement. Darknet marketplaces are no different. Because vendors almost exclusively accept virtual currency as payment, we can sometimes identify the vendors based solely on their transactions. The vendors generally convert between traditional currency and virtual currency, which provides an extra data point that may be available to law enforcement via the exchangers. This data point is generally not obtainable in traditional sales of illicit items.

Furthermore, the semi-anonymous nature of virtual currency transactions also enables the FBI to more easily conceal covert investigations targeting unlawful actors.

Obstacles Presented by Illicit Use of Virtual Currency

While the illicit use of virtual currency can provide additional breaching points for our investigations, it can present challenges as well. During the Committee's June 8, 2017 hearing on virtual currency, all of the witnesses and several Members identified current and potential hurdles in identifying and neutralizing actors who conceal their crimes using virtual currency. These obstacles include

1. The illicit use of virtual currencies that have anonymous ledgers and blockchains;

2. The use of virtual currency exchangers and mixers that are unresponsive to law enforcement requests;
3. The exchange of virtual currency via uncooperative nation-states' centralized currencies or electronic payment systems;
4. Concerns over the training, familiarity, and aptitude of law enforcement personnel in combating these issues; and
5. The general efficiency and bureaucratic-related challenges of working multi-national investigations.

FBI Response to Obstacles Presented by the Illicit Use of Virtual Currency

Illicit Use of Virtual Currencies with Anonymous Ledgers and Blockchains

Anonymity-enhanced virtual currencies can be difficult to decipher and unscramble. While some anonymous virtual currencies are more complex than others to unwind, they all have one common attribute: the goal of anonymity.

Obtaining and transacting in these anonymous virtual currencies can be a red flag, both for law enforcement and for private entities that accept and exchange anonymous virtual currencies. However, a criminal investigation would not be solely predicated on an actor's use of anonymity-enhanced virtual currency. While the possession of anonymity-enhanced virtual currency is not by itself illegal, when viewed with other evidence of a crime, this anonymity may well tend to support the idea that an actor intended to commit (or has committed) a crime. Private entities have provided the FBI with records of suspected illicit actors using anonymous virtual currencies based on mandatory reporting requirements, on responses to official requests, and sometimes on proactive, voluntary engagement. By constantly engaging with private industry, the FBI is able to partner with industry to reveal the users of virtual currency, both public and anonymous.

The Use of Virtual Currency Money Transmitters and Mixers that are Unresponsive to Law Enforcement Requests

There are certain virtual currency money transmitters, mixers, and tumblers that are unresponsive to official government requests from the United States. Particularly in the case of mixers and tumbler, we often do not know where in the world these entities reside.

However, there are steps the FBI can take to mitigate a lack of cooperation. First, when we do know where an entity is based, we can attempt to work directly with that country's law enforcement. Even certain countries, for which one would not expect cooperation, sometimes do cooperate.

Moreover, subject entities sometimes maintain resources and/or equipment outside of the uncooperative host country. For example, if an uncooperative mixer is located in an uncooperative country but maintains servers, bank accounts, or other equipment or personnel

within cooperative countries, law enforcement can leverage those situations within the cooperative country.

Finally, the FBI can use tools to analyze transactions regardless of where the exchange, mixing, or tumbling service is located. While geographic boundaries limit what can be accomplished physically in uncooperative territories, the very nature of virtual currency provides a boundary-less electronic footprint to scrutinize. While it is much more favorable to have cooperation from these services and their host countries, there are still opportunities to track and identify illegal conduct even when cooperation is lacking.

The Exchange of Virtual currency via Uncooperative Nation-States' Centralized Currencies or Electronic Payment Systems

During the Committee's June 8, 2017 hearing, multiple witnesses spoke about the potential for criminal actors to launder proceeds of their conduct by using electronic currency and payment systems that are based in foreign countries. Specifically, the Russian exchange service "WebMoney" and Chinese payments services "AliPay" and "WeChat Pay" were mentioned. Criminals—particularly those engaged in cyber-enabled criminal conduct—still use services like WebMoney. In addition, these criminals often exchange Bitcoin: which creates a double challenge for law enforcement. If these companies are located in foreign countries, the FBI can make a mutual legal assistance treaty ("MLAT") request, but this is typically not an expeditious process.

Criminals are nearly always early adopters of new technologies and these centralized systems were the first virtual currencies the FBI saw criminals exploit. Although the invention of decentralized virtual currencies, like Bitcoin, changed the financial landscape, centralized systems have found ways to incorporate decentralized currencies into their existing business models and criminals continue to exploit them.

Concerns over the Training, Familiarity, and Aptitude of Law Enforcement Personnel in Combating these Issues

Another concern is law enforcement's inability to learn, understand, and investigate virtual currency-linked criminal conduct. At the FBI we feel solidly equipped to tackle virtual currency developments and continually work to increase our familiarity with and knowledge of these issues. For example, FBI investigators have an understanding of the Automated Clearing House ("ACH") payments system, financial institutions' debiting and clearing systems, and credit card processing systems, and are excellent at requesting and scrutinizing the records of those respective transactions. Today, as financial transacting has evolved, the FBI continues to build expertise, now in virtual currencies, exchange systems, and the like, to equip our investigators to address these new challenges with the same level of expertise and effectiveness.

In addition, the FBI leverages analytical tools to exploit data on the blockchain to trace virtual currency transactions and follow the money to identify targets. In fiscal year 2017,

through its Virtual Currency Initiative, the FBI's Money Laundering, Forfeiture, and Bank Fraud Unit ("MFBU") as well as the National Cyber Investigative Joint Task Force's ("NCIJTF") Virtual Currency Team ("VCT") trained approximately 1,900 FBI employees regarding the description, identification, tracing, unmasking, and seizing of virtual currencies. Trainings ranged between two hour online classes to concentrated, multi-day conferences featuring industry experts and international law enforcement partners.

The FBI has also teamed with other valued law enforcement and private industry partners in several task forces in Washington, D.C., and throughout the country, in order to combine resources, leverage expertise, and identify best practices.

Currently, the FBI has over 100 open investigations relating to the use of virtual currencies. These investigations are focused on money laundering, cyber intrusion, business email compromise, securities fraud, initial coin offerings, human trafficking, drug trafficking, and bank fraud. The investigations are being worked out of roughly 30 different field offices, and each has received assistance from virtual currency subject matter experts located within FBI Headquarters. Most of the investigations are multi-State, and many are multi-national.

In fiscal year 2018 to date, FBI investigations have led to the seizure of virtual currency worth approximately $60,000,000, aggregated among approximately 30 different investigations. These assets were either used in furtherance of illicit conduct or were the proceeds of illicit conduct.

In the last couple years, the FBI and its law enforcement partners have taken down large Darknet marketplaces, identified hundreds of illicit actors using virtual currencies, and arrested dozens of individuals using virtual currencies. The FBI and its domestic and foreign partners are deconflicting some of the highest priority targets and will continue to work in tandem into the future.

The General Efficiency and Bureaucratic-related Challenges of Working Multi-National Investigations

All multi-agency and multi-national investigations have bureaucratic inefficiencies. Unfortunately, these inefficiencies appear unavoidable as each agency has disparate protocols and approvals required to work cross-programmatic, multi-agency, and multi-national investigations.

As stated above, one benefit the FBI and its law enforcement partners have in combating crimes involving virtual currency (in contrast to investigations involving traditional currency) is the existence of many standing joint task forces and ongoing multi-national relationships that foster cooperation in virtual currency investigations. For example, the FBI partners with several other Federal law enforcement agencies within the NCIJTF.

The NCIJTF has ongoing coordination with several local, State, and foreign law enforcement agencies. Therefore, for example, when a Sacramento-based FBI investigation requires the production of records from an Amsterdam-based entity, the NCIJTF can quickly contact the Dutch police (if they are not involved already), and the Dutch police can iron out the record production process locally. Because of the multi-national reach of most investigations involving virtual currency, the FBI must cultivate and maintain outstanding relationships across jurisdictions and venues.

One final challenge worth mentioning seems to be the easiest to remedy — although Federal regulation establishes anti-money laundering standards that apply to virtual currency companies, the State regulatory environment surrounding virtual currency creates a complex environment for investigators, particularly State and local partners, to navigate. Each State has its own separate and unique legal, regulatory, and licensing requirements surrounding virtual currency and money transmission. These requirements are separate from the Federal system and subject to unique interpretation from each State's court system. Nevertheless, Federal law and regulations (including accompanying interpretive guidance) make clear that virtual currency money transmitters, including most if not all so-called "administrators" and "exchangers" of virtual currency are regulated under Federal law, and those who operate illegally can be charged under Federal money laundering statutes. Additionally, Federal courts have held that virtual currency constitutes "funds" for purposes of the Federal money laundering statues and the Federal statute that prohibits unlicensed money transmitting businesses (18 U.S.C. § 1960).

Conclusion

I want to reiterate the FBI's commitment to combating the threats posed by the illicit use of virtual currency and our dedication to evolving alongside this rapidly changing technology. Through continued partnerships with private industry and with our foreign and domestic law enforcement partners, the FBI will continue to fight to protect the American people from illicit actors using virtual currency.

Thank you very much for your time and consideration.

Questions for the Record
"Illicit Use of Virtual Currency and the Law Enforcement Response" TIF Hearing
Wednesday, June 20th at 2:00 pm
Congresswoman Krysten Sinema

All questions directed to Mr. Thomas P. Ott, Associate Director, Enforcement Division, of the Financial Crimes Enforcement Network (FinCEN).

1. **Your testimony indicates that virtual currency transactions include billions of dollars obtained through ransomware extortion and hacks of virtual currency exchanges. It also notes Suspicious Activity Reporting (SAR) filings concerning virtual currencies increased 90 percent from 2016 to 2017. While it is good to hear that these filings have been useful for specific criminal and civil investigations, it is also important that we analyze SAR filings to create intelligence products and guidance that help financial institutions deter and choke off future illicit activity. What work has FinCEN, in coordination with appropriate law enforcement and intelligence agencies, done to advance this effort in the fast-evolving world of virtual currencies?**

   Answer: FinCEN is proud to have some of the foremost subject matter experts on virtual currency in the U.S. government. This helps us use our vast amounts of financial intelligence to help target illicit activity and identify new criminal methodologies. FinCEN disseminates intelligence assessments and reports to law enforcement, the intelligence community, and other government partners to help improve understanding of virtual currency typologies and where there may be illicit activity to target. FinCEN also supports law enforcement and other investigations directly by providing analysis or subject matter expertise, most often in the form of investigative reports and requests for information responses. We interact daily with our law enforcement counterparts, and FinCEN hosts liaisons from ten different law enforcement agencies to support our common missions.

   In addition to producing reports, FinCEN has played an active role in providing briefings and training to different partner agencies across government. In Fiscal Year 2018, FinCEN conducted over 20 presentations and trainings, reaching more than 1,000 staff from federal and state regulatory and law enforcement agencies.

   FinCEN's regulations under the Bank Secrecy Act (BSA) set the framework for combating money laundering and illicit activity promoted through the use of virtual currency. FinCEN issued guidance in 2013 and a series of administrative rulings to clarify to financial institutions and other stakeholders the applicability of anti-money laundering and combating the financing of terrorism (AML/CFT) regulations under the BSA to specific virtual currency-related business models and activities. Under this framework, virtual currency exchanges and administrators must, among other AML/CFT obligations, report on suspicious transactions involving virtual currency use in suspicious activity reports (SARs). FinCEN

leverages this reporting by financial institutions in our intelligence assessments and law enforcement support, as described above. Additionally, FinCEN conducts compliance examinations of virtual currency businesses operating as Money Services Businesses that help ensure they are adequately prepared to handle AML/CFT challenges, specifically in highlighting deficiencies that can be corrected to build better resilience at financial institutions against AML/CFT risks.

To enhance SAR reporting by financial institutions, FinCEN can also issue advisories that alert the financial sector to typologies of illicit activity and methods, such as keywords, to more easily identify the reporting of such activity to FinCEN and law enforcement stakeholders. FinCEN issued an advisory in 2016 alerting the sector to the need to report cyber-related financial crimes and provide technical indicators, including involved virtual currency addresses, connected with suspicious transactions in SAR reporting. FinCEN's October 2018 advisory on Iran's attempts to exploit the financial system also flagged for financial institutions Iran's potential interest in virtual currency use as a means to evade sanctions. FinCEN also maintains constant outreach with industry and participation in financial conferences, including engagement through the BSA Advisory Group, to increase understanding across financial institutions of the nature of virtual currency technologies and activities, their AML/CFT regulatory obligations, and trends and typologies in their use to support criminal activity.

Finally, FinCEN uses SARs and other filings by financial institutions to develop its own investigations as well. FinCEN has taken several actions against non-compliant virtual currency financial institutions over the past several years including Liberty Reserve (2013), Ripple Labs (2015), and BTC-e (2017). Each of these actions were parallel criminal and civil proceedings coordinated with law enforcement, and each case benefited from information provided by U.S. financial institutions.

2. **An important consideration as we establish methods to stop illicit activity on virtual currency exchanges is how much anonymity is afforded to users. Those who misuse virtual currency for illicit purposes generally rely on anonymity to cover their tracks. How often are illicit transactions from American virtual currency exchanges untraceable?**

Answer: FinCEN shares your concerns over the anonymity provided by some virtual currencies. To that end, FinCEN has been at the forefront of highlighting these concerns to investigators across government. As I noted in my testimony, anonymity-enhanced cryptocurrencies (AECs)—sometimes referred to as "privacy coins"—are increasingly prevalent across exchange platforms and average around $300 million in daily transaction volume at domestic and foreign-located exchanges. Importantly, FinCEN has asserted that financial institutions that offer AECs have the same responsibilities under Anti-Money Laundering (AML) laws as other virtual currencies. That means that a financial institution offering an AEC would still have to implement an AML program and have policies and procedures to mitigate risk, and, as appropriate, file suspicious activity reports.

FinCEN's virtual currency experts have been studying many of these AECs and are working across government to analyze and assess this activity. FinCEN would be happy to provide more details in a closed setting. We defer to our colleagues in federal law enforcement who are better placed to discuss how often AECs appear in their investigations.

○